# Digitaalinen identiteettilompakko ja sähköisen tunnistamisen tulevaisuus

Diplomityö
Turun yliopisto
Tietotekniikan laitos
Ohjelmistotekniikka
2022
Juho Kronbäck

TURUN YLIOPISTO
Tietotekniikan laitos

Juho Kronbäck: Digitaalinen identiteettilompakko ja sähköisen tunnistamisen tulevaisuus

Diplomityö, 86 s.
Ohjelmistotekniikka
Joulukuu 2022

---

Tässä työssä vertaillaan vahvan sähköisen tunnistautumisen nykytilannetta Suomessa alan tulevaisuuden näkymiin. Välttämättömien perustietojen käsittely johtaa Finnish Trust Network (FTN)-järjestelmän käsittelyyn, joka toimii työssä nykypäivän vertailukohteena. Työssä tutkitaan FTN-järjestelmästä löytyviä puutteita ja haasteita, joita peilataan tulevaisuuden vertailukohdetta vastaan. Tämän roolin työssä ottaa EU:n digitaalinen identiteettilompakko. Työssä käsitellään yksi identiteettilompakon referenssiratkaisu, jonka on tuottanut työnantajani Gurulogic Microsystems Oy. Lisäksi esitetään käytännön huomioita identiteettilompakon käyttöön liittyen. Työn yhteydessä pidettiin kyselytutkimus, jolla haetaan potentiaalisten käyttäjien mielipiteitä identiteettilompakkoon ja sen ominaisuuksiin liittyen. Tutkimus perustuu kirjalliseen analyysiin kustakin työn aihepiiristä, käytännön havainnointiin ja kokemukseen referenssiratkaisua tuottavasta yrityksestä sekä kyselytutkimuksen lopputulosten analyysiin. Työn lopputuloksena todetaan, että identiteettilompakkoratkaisu kykenee vastaamaan nykyisessä FTN-järjestelmässä ilmeneviin ongelmiin ja täten edistää vahvan sähköisen tunnistautumisen alaa.

Asiasanat: identiteettilompakko, EUDIW, Finnish Trust Network, sähköinen tunnistaminen, digitaalinen henkilöllisyys

UNIVERSITY OF TURKU
Department of Computing

Juho Kronbäck: Digitaalinen identiteettilompakko ja sähköisen tunnistamisen tulevaisuus

Master of Science Thesis, 86 p.
Software Engineering
December 2022

---

This thesis concerns the current status of electronic identification services in Finland and compares it to the future prospects of the industry. Coverage of basic concepts leads into exploration of the Finnish Trust Network (FTN)-service, which functions as the current day identification broker of the thesis. The system is analyzed for potential problems that could be solved by future methods. This role is taken by the upcoming European digital identity wallet, which is covered in detail alongside one reference solution produced by my employer, Gurulogic Microsystems Oy. Practical considerations of using such systems are explored. During the thesis writing process, a survey was held which aims to map out how potential users of the product see the wallet and its features. The thesis is based on literary analysis of each major topic, on practical experience obtained during the course of my employment at Gurulogic Microsystems Oy and on analysis of the survey results. The research finds that the identity wallet can solve the problems found in Finnish Trust Network and thus can progress the field of electronic identification.

Keywords: digital identity wallet, EUDIW, Finnish Trust Network, electronic identification, digital identity

# Sisällys

# Kuvat

# Taulukot

# 1 Johdanto

Vahva sähköinen tunnistautuminen on nykyajan keksintö, jonka yhteiskunnallinen merkitys kasvaa jatkuvasti. Ilman vahvaa sähköistä tunnistautumista verkossa toimivien palveluiden käyttäjien henkilöllisyyden varmistaminen ei olisi mahdollista, eikä arkaluontoisia tietoja koskeva sähköinen asiointi olisi turvallista, palvelun maksullisuudesta riippumatta. Palveluntarjoajalla ja erityisesti palvelun käyttäjällä on selkeä tietosuojaintressi, jonka seurauksena molemmat osapuolet haluavat varmistaa sähköistä palvelua käyttävän henkilön henkilöllisyyden vahvan sähköisen tunnistamisen avulla. Tämä työ käsittelee digitaalista henkilöllisyyttä ja sähköisen asioinnin tulevaisuutta erityisesti eurooppalaisen identiteettilompakon näkökulmasta, joka on tuleva kansainvälisesti implementoitava sähköinen tunnistautumisratkaisu sähköisten palveluiden käyttöön. Tämän työn ensimmäisissä kappaleissa esitellään perusteet digitaaliselle identiteetille ja digitaaliselle tunnistamiselle sekä nykyaikaisen Finnish Trust Network (FTN)-järjestelmän toiminta, rakenne, puutteet ja ongelmat. Neljännessä ja viidennessä kappaleessa esitellään uusi järjestelmä, sen ominaisuudet, sekä eräs mahdollinen kandidaatti sen toteuttamiseen. Näissä kappaleissa analysoidaan kirjallisesti, miten tuleva ratkaisisi nykyaikaisesta järjestelmästä löytyneet puutteet. Kuudennessa kappaleessa esitetään työn ohessa suoritettu mielipidekysely, jossa kuutta osanottajaa pyydettiin ottamaan kantaa uusien sekä nykyisten sähköisten tunnistautumispalveluiden ominaisuuksiin. Työn löydökset perustuvat erityisesti kirjalliseen tutkimukseen, mutta myös käytännön havainnointiin referenssi-

ratkaisua kehittävässä yrityksessä. Työn yhteydessä pidetyn kyselyn lopputulokset lisäävät tutkimukseen empiirisen kulman. Tämä työ tuotettiin yhteistyössä Gurulogic Microsystems Oy:n kanssa, joka työstää sovellustason ratkaisua eurooppalaisen identiteettilompakon tarpeisiin. Tämä ratkaisu esitetään kappaleessa 5.

Tutkimuksessa on neljä pääkysymystä, jotka ovat seuraavat:

1. Miksi tarvitaan digitaalinen identiteetinhallinta- ja lompakko-ohjelmisto?
2. Mitkä tekijät täytyy huomioida, että ohjelmiston käyttäjäkokemus voidaan kehittää nykyratkaisuja paremmaksi?
3. Miten ohjelmisto julkaistaan nykyisten ratkaisujen ohelle siten, että siihen siirtyminen hyödyttää loppukäyttäjää?
4. Miten yksi identiteetinhallintasovellus kattaa sille olennaiset käyttötapaukset? Voidaanko keksiä uusia käyttötapauksia?

Puhtaasti tieteellisestä näkökulmasta katsottuna tämän työn tavoitteena on digitaalisten identiteetinhallinta- ja tunnistautumissovellusten haasteiden, ominaisuuksien ja käyttötapauksien tutkiminen ja dokumentaatio. Erityistä huomiota kiinnitetään siihen, miten tulevaisuuden tunnistautumisratkaisujen tulisi vastata nykyaikaisissa järjestelmissä oleviin ongelmiin. Haluan kiittää lukijaa mielenkiinnosta, Gurulogic Microsystems Oy:tä yhteistyöstä, työnohjaajia loistavasta työstä ja maltillisuudesta, sekä kaikkia tuttuja, jotka omilla tavoillaan auttoivat tätä työtä eteenpäin tämän pitkän projektin aikana. Nautinnollisia lukuhetkiä!

# 2 Fyysinen ja digitaalinen identiteetti

Yksilön identiteetin määritelmä on pohjimmiltaan yksi ihmiskunnan vanhimmista filosofisista kysymyksistä, johon suuret filosofit ovat etsineet vastausta jo aikojen alusta asti [1]. Identiteetti perustuu henkilön omakuvaan, eli omaan näkemykseen itsestään, johon perustuvaa identiteettiä voidaan kutsua psykologiseksi identiteetiksi, koska se on omistajansa psykologisen tilan määrittelemä [2]. Muuttuva, monimutkainen ja yksilön sisäinen psykologinen identiteetti ei kuitenkaan ole ulkoisesti varmennettavissa, joten se ei sovellu tilanteeseen, jossa arvovaltaisen tahon täytyy erottaa kaksi yksilöä toisistaan. Identiteettiä tarkastellaan tällöin yksilön ulkopuolisesta näkökulmasta, tarkoituksena muodostaa kummallekin yksilöllinen identiteetti ulkoisesti varmennettavien ominaisuuksien perusteella [2]. Tästä voidaan käyttää nimeä sosiaalinen identiteetti, jonka perusteella yhteiskunnan jäsen erottaa hänet yhteiskunnan muista jäsenistä [3]. Arkielämässä sosiaalisen identiteetin hallinta on intuitiivinen prosessi, jossa kukin yhteisön (esim. ystäväpiirin, perheen tai työyhteisön) jäsen tunnistaa muut jäsenet vaivattomasti [4] ihmiselle luontaisia taitoja hyödyntäen [5]. Nämä identiteetin ulottuvuudet voidaan tiivistää yhteen sanaan, joka käsittää identiteetin omistajan koko olemuksen todellisessa maailmassa. Tässä työssä tätä käsitettä kutsutaan nimellä "fyysinen identiteetti", joka tarkoittaa henkilön identiteettiä fyysisessä maailmassa. Fyysisen ulottuvuuden lisäksi yksilön identitee-

tin käsite pätee myös digitaalisessa ulottuvuudessa, jossa ulkoisesti varmennettavat ominaisuudet ovat erilaisia kuin fyysisessä maailmassa. Tätä voidaan vastaavasti kutsua nimellä "digitaalinen identiteetti", joka tarkoittaa identiteettiä digitaalisessa maailmassa. Kullakin yksilöllä on ainutlaatuinen fyysinen identiteetti. Yksilön fyysinen identiteetti on kiteytetty valtion (esim. poliisilaitoksen) myöntämään henkilöllisyystodistukseen, jonka perusteella viranomainen voi varmistaa todistuksen omistajan henkilöllisyyden todistuksessa annettujen ulkoisesti varmennettavien tietojen perusteella, joihin lukeutuu mm. passikuva ja sosiaaliturvatunnus [6].

Fyysiseen identiteettiin verrattuna digitaalinen identiteetti voidaan nähdä ihmiskunnan keksintönä, mutta käytännössä sitä voidaan pitää nykyaikaisen teknologiayhteiskunnan ratkaisujen mahdollistamana fyysisen identiteetin ilmentymänä digitaalisessa ulottuvuudessa. Fyysisestä identiteetistä poiketen digitaalinen identiteetti ei synny automaattisesti sen kohdeyksilön syntymän yhteydessä, vaan se täytyy erikseen luoda henkilön tai laitteen toimesta [7]. Ennen Internetin syntyä digitaalisen identiteetin tarve oli matala, mutta tarve sille ja sen hallinnalle on ollut selkeässä nousussa jo vuosituhannen vaihteesta alkaen [8]. Digitaalinen identiteetti on noussut merkittävään asemaan nyky-yhteiskunnassa mm. sosiaalisen median palveluiden johdosta [9]. Esimerkiksi presidenttien, poliitikkojen ja muiden julkisuuden henkilöiden kannat, asenteet ja mielipiteet nousevat esille julkisesti luettavina viesteinä sosiaalisen median palveluissa [10]. Nämä viestit sekä niiden sisältö ja merkitys sidotaan sen kirjoittaneen henkilön digitaaliseen identiteettiin. Jos viesti vaikuttaa positiivisesti tai negatiivisesti digitaalisen identiteetin imagoon, se voi vaikuttaa kirjoittajan imagoon myös fyysisessä maailmassa [9]. Sosiaalisen median palveluiden käyttäjät luottavat siihen, että muiden käyttäjien sähköiset profiilit vastaavat heidän fyysisiä identiteettejään ja että käyttäjät eivät kirjoita viestejä palveluun toisten henkilöiden nimissä. Tämä on tärkeä edellytys, koska ainoastaan siihen perustuen voidaan olettaa, että profiilin omistajat ovat vastuussa heidän palstoillaan olevis-

ta viesteistä sekä niiden sisällöstä. On tärkeää huomata, että yksilön digitaalinen identiteetti on kaikenkattava, se sisältää kaiken digitaalisen sisällön, jonka kohde on luonut tai joka on kohteelle luotu, mukaan lukien erilaisten nettisivustojen ja sosiaalisten median palveluiden käyttäjätilit ja niiden sisällöt [9].

Digitaalinen identiteettivarkaus toimii tehokkaana esimerkkinä fyysisten ja digitaalisten identiteettien välisestä riippuvuudesta. Matti Meikäläinen omistaa Canon-monitoimitulostimen. Tulostimen oston yhteydessä hän on luonut profiilin sivustolle `www.usa.canon.com`. Profiili on suojattu sähköpostiosoitteella ja salasanalla [11]. Näiden tunnusten varastamisen tulisi mahdollistaa pääsy ainoastaan Canonin kotisivujen toimintoihin Matin käyttäjätilillä, erityisesti jos Matti ei käytä samaa salasanaa sivustojen välillä. Varkauden yhteydessä paljastunut sähköpostiosoite kuitenkin avaa mahdollisuuden siihen, että varas rikkoo kyseisen sähköpostitilin salasanan, jolloin hän pystyy lukemaan Matin henkilökohtaisia sähköposteja sekä lähettämään viestejä hänen nimissään. Tässä pisteessä huomattavasti Canonin kotisivuja suurempi osa Matin digitaalisesta identiteetistä on joutunut vääriin käsiin [9]. Varas pystyy seuraamaan ja vaikuttamaan hänen digitaaliseen aktiivisuuteensa sähköpostitilin välityksellä. Kysymys kuuluu, kuinka vaikutusvaltainen tämä sähköpostiosoite on ja kuinka kauan identiteettivaras pystyy käyttämään sitä? Varastettujen attribuuttien määrän kasvaessa identiteettivaras pystyy lopulta tekemään ostoksia ja solmimaan sopimuksia Matin digitaalisen identiteetin nimissä, jotka voivat vaikuttaa hänen hyvinvointiinsa myös digitaalisen maailman ulkopuolella esim. Matin kotiovelle saapuvien laskujen ja velvoitteiden tai maineen menetyksen muodossa [12]. Sisältääkö Matin sähköpostitili esim. arkaluontoisia tietoja, joiden avulla identiteettivaras voi kiristää Mattia ja/tai hänen perheenjäseniään nyt ja tulevaisuudessa [13]? Mahdollistaako tiedetty sähköpostiosoite pääsyn Matin sosiaalisen median palveluihin ja tätä kautta julkisten viestien kirjoittamiseen Matin nimissä? Onko Matti julkisuuden henkilö tai päättävässä asemassa oleva henkilö, toisin sanoen, vaikuttaako

hänen asemansa hänen nimissään kirjoitettujen viestien vaikutus- ja päätäntävaltaan? Jokainen Matille kuuluva sähköinen tili on hänen digitaalisen identiteettinsä ominaisuus, joista osa vastaa Matin fyysistä identiteettiä vahvemmin kuin toiset [14]. Sähköpostiosoite on tyypillisesti tämän hierarkian merkittävässä päässä, mutta kaikkein vahvimpia sähköisiä tunnisteita, kuten verkkopankkitunnuksia, käytetään polettina käyttäjän fyysisen identiteetin suorana vastineena. Tämän tason tunnuksilla voidaan tehdä ostoksia lähes kaikkialla internetissä sekä niiden perusteella sovitaan ja valtuutetaan elämää muuttavia sopimuksia. Voidaan todeta, että digitaalisen identiteetin väärinkäyttö voi johtaa vakaviin ja mahdollisesti peruuttamattomiin seurauksiin uhrin sähköisessä sekä todellisessa elämässä [12][13]. [15]

Fyysisten ja digitaalisten identiteettien asteittainen yhdistyminen nyky-yhteiskunnassa tuottaa uusia haasteita identiteetinhallinnan alalla. Elämme murrosvaiheessa, jossa kummankin tyyppisiä identiteettejä hyödynnetään yhtäaikaisesti. Identiteetin käyttö yhteiskunnassa perustuu siihen, että valtuutusta pyytävä viranomainen pystyy tarkistamaan hakijan henkilöllisyyden helposti ja toimintavarmasti; toimenpide, joka muuttuu fyysisen ja digitaalisen ulottuvuuden välillä. Tyypillisesti fyysinen identiteetti osoitetaan valtion myöntämällä kuvallisella henkilöllisyystodistuksella, ajokortilla tai passilla esim. alkoholijuomia ostettaessa tai pankkiasioinnin yhteydessä [6]. Fyysisen identiteetin osoittaminen vieraiden ihmisten välillä perustuu siis suuresti valtion myöntämään henkilöllisyystodistukseen. Nykyaikaiset henkilöllisyystodistukset ovat kuvallisia, jolloin valtuutuksessa voidaan hyödyntää ihmiselle luontaisia kasvontunnistustaitoja [5]. Kuvan perusteella viranomainen näkee, että henkilöllisyyttään todistava henkilö ja henkilöllisyystodistuksessa esitetty henkilö vastaavat toisiaan, mikä edistää tarkastuksen nopeutta ja toimintavarmuutta. Ajokortissa oleva kuva on ainoa kortissa annettu tieto, jonka oikeellisuus on nopeasti varmennettavissa, mutta myös muita kortissa annettuja tietoja, kuten sosiaaliturvatunnusta [6], voidaan hyödyntää tarpeen vaatiessa. Kokonaisuudessaan voidaan

sanoa, että fyysisen identiteetin tarkistaminen on ihmiskeskeinen prosessi, jossa ihminen toimii hakijana ja tarkastajana. Digitaalisen identiteetin tarkastaminen ei ole ihmiskeskeinen prosessi, vaan kahden laitteen välinen prosessi. Digitaalista identiteettiä varmennettaessa virkamiehen järjestelmä pyytää tunnistetiedon kohdejärjestelmältä. Jos tunnistetieto ei ole käyttäjän syöte, kuten sähköinen kulkukortti, hakijan täytyy ainoastaan asettaa se lukijaan, joka lukee tunnistetiedon kortin sisältä ja hyväksyy tai hylkää sen. Jos tunnistetieto on käyttäjän syöte, kuten sovittu käyttäjätunnus/salasanapari, PIN-koodi tai (kohteen) silmän iiriksen skannaus, käyttäjän täytyy syöttää tieto laitteeseen, joka välitetään valtuuttavalle järjestelmälle joka hyväksyy tai hylkää sen. Kummassakin tapauksessa tunnistautumisen osapuolet ovat laitteita, jotka käsittelevät puhtaasti digitaalista tai käyttäjän syötteestä digitalisoitua tietoa.

## 2.1 Identiteetin määrittävä informaatio

Hallitakseen identiteettiä identiteetin omistajan täytyy pystyä vakuuttamaan identiteetin tarkastaja missä ja milloin tahansa, eli hänen täytyy hallita identiteetin määrittävää informaatiota. Tästä syystä suuri osa aikuisista ihmisistä kantaa jonkinlaista henkilöllisyystodistusta mukanaan kokoaikaisesti [16]. Fyysisen identiteetin määrittävää informaatiota löytyy henkilöllisyystodistuksen lisäksi myös sen ulkopuolelta. Itse asiassa yksilön koko olemus määrittelee hänen fyysisen identiteettinsä aina biometrisistä ominaisuuksista, kuten iiriksestä ja kasvoista [17], attribuutteihin, kuten minkälaisia värähtelyjä hänen jalanjälkensä tuottavat maaperässä [18]. Näiden ominaisuuksien väärentämisen, esittämisen ja tarkistamisen vaikeustaso vaihtelee helposta mahdottomaan, tehden joistain ominaisuuksista erityisen luotettavia. Identiteetin määrittävä informaatio voidaan jakaa seuraavasti:

- Taso 1: Biometrinen identiteetti

Yksilön biometrinen ominaisuus on yleensä synnynnäinen, lähes muuttumaton ja ainutlaatuinen kehon fyysinen muodostuma. Biometrisiin ominaisuuksiin lukeutuu mm. kasvonpiirteet, sormenjäljet, ääni, iiris, askellaji, pysyvät arvet sekä allekirjoitus [19]. Täydellisiä kaksosia lukuun ottamatta biometristen ominaisuuksien matkiminen on erittäin vaikeaa tai mahdotonta, mikä mahdollistaa äärimmäisen vahvojen tunnstautumiskeinojen kehittämisen sillä edellytyksellä, että identiteetin omistaja on fyysisesti paikalla. Biometristen ominaisuuksien yksityiskohtaisuuden vuoksi tarkastus tapahtuu yleensä koneellisesti [20], mutta esim. silmien väri voidaan todentaa paljaalla silmällä. [4]

- Taso 2: Jaettu identiteetti

  Tämän taso koostuu identiteeteistä, jotka solmitaan kohteen (=identiteetin omistajan) ja arvovaltaisten tahojen kesken. Sovitun sopimuksen perusteella kohde omistaa oikeuden jaetun identiteetin käyttöön arvovaltaisen tahon valtuuttamana. Valtion myöntämä ajokortti, passi ja henkilöllisyystodistus, pankin myöntämä luottokortti, yrityksen myöntämä toimikortti ja käyttäjän internetissä luoma profiili ovat tyypillisiä toisen tason identiteettejä. Nimitys "jaettu identiteetti"perustuu siihen, että jos kumpikaan osapuoli peruu keskinäisen sopimuksen, heidän välinen jaettu identiteetti raukeaa. [4]

- Taso 3: Sovellettu identiteetti

  Sovellettu identiteetti muodostetaan kohteen attribuutteja yhdistelemällä. Menetelmä tunnistaa kohteen välillisesti ja yksilöi kohteen muista. Esimerkiksi nimet, iät, kotiosoitteet, puhelinnumerot ja sähköpostiosoitteet ovat yhdisteltäviä attribuutteja. Esimerkiksi attribuutit "yli 90-vuotias", "nainen", "Helsinki"ja "purjeveneen omistaja"muodostavat sovelletun identiteetin, joka rajaa potentiaalisten kohteiden määrän hyvin pieneksi [21]. [4]

Sen lisäksi, että identiteetin määrittävä informaatio voidaan jakaa luotettavuuden perusteella, se voidaan jakaa myös tyypin perusteella [22, p. 5]:

- Tunnisteet

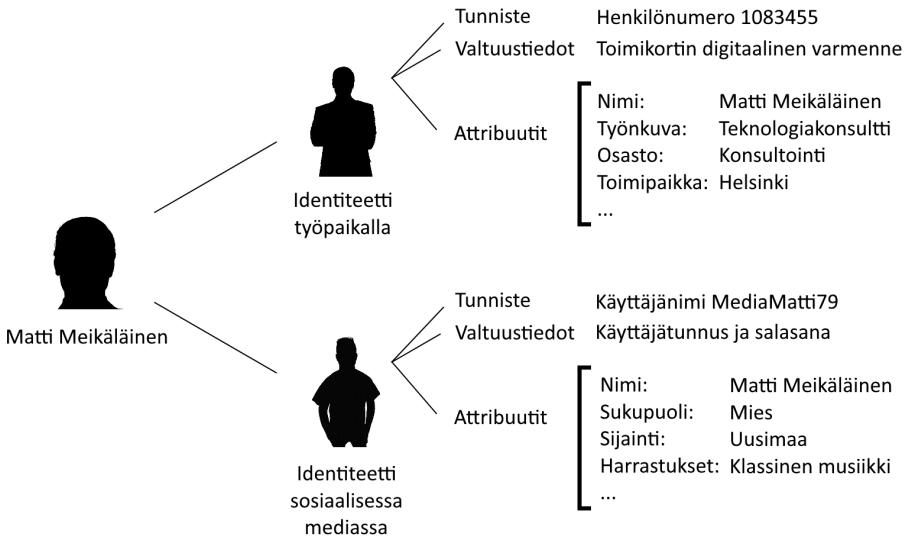
  Tunnisteet ovat kohteelle yksilöllisiä numero-, merkki- ja symbolisarjoja. Esimerkiksi URL:t, sähköpostiosoitteet, puhelinnumerot ja IP-osoitteet ovat tunnisteita [22, p. 5]. Tunniste voi olla globaali, eli muuttumaton useiden organisaatioiden välillä (esim. sähköpostiosoite), pseudonyymi, kuten käyttäjänimi foorumilla, joka voi toistua eri organisaatioiden välillä, tai kertakäyttöinen tunniste, jolla on sovittu aika- tai käyttörajoitus [22, p. 15]. Esimerkiksi prepaid-liittymän puhelinnumero on kertakäyttöinen tunniste, joka pätee ainoastaan liittymän loppuun asti.

- Valtuustiedot

  Tämän tyyppinen informaatio on kohteen valtuuttavaa informaatiota, johon lukeutuu mm. käyttäjätunnus/salasanaparit, digitaaliset sertifikaatit, kulkuluvat ja -kortit, älykortit ja biotunnisteet. Valtuustieto mahdollistaa kohteen oikeuksien osoittamisen ja varmentamisen. Valtuustiedon myöntäjä voi tyypillisesti purkaa valtuuden esim. väärinkäytön seurauksena. [22, p. 16]

- Attribuutit

  Attribuutit ovat kohdetta kuvailevaa informaatiota, jonka avulla kohteen ominaisuudet määritellään. Attribuuttien perusteella kohteelle voidaan muodostaa sovellettu identiteetti. Attribuutit voivat myös sisältää erilaisia oikeuksia, rajoitteita ja tilannekohtaisia tietoja, kuten pelissä ajettujen kilometrien määrän. [22, p. 15]




Kuva 2.1: Identiteetin määrittävä informaatio [23, kuva 2.1, piirretty uudestaan]

Kuvassa 2.1 esitetään, miten kohteen identiteetti muodostuu eri luokkiin jaoteltavasta informaatiosta. Matin identiteetti voidaan purkaa sen määrittävään informaatioon abstraktiotaso kerrallaan. Jos Matin identiteetti pyritään muodostamaan sen määrittävän informaation perusteella, eli purkuprosessi peruutetaan, Matti Meikäläisen todellisen identiteetin muodostaminen ei ole mahdollista, koska identiteetin määrittävää informaatiota yhdistelemällä pystytään muodostamaan ainoastaan sovellettu identiteetti [4]. Tästä puutteesta huolimatta identiteetin määrittävän informaation hallinnan menettäminen on vaarallista, koska se sisältää valtuustietoja. Tiedon vääriin käsiin joutuminen aiheuttaa vaaratilanteita, joiden syntymisen ennaltaehkäisemiseksi voidaan käyttää apuna identiteetinhallintaa (IAM = Identity Access Management) [24].

### 2.1.1 Ydinidentiteetti (PID/PII)

Vahvan sähköisen tunnistautumisen alan kontekstissa identiteetin määrittävä informaatio voidaan usein tiivistää ydinidentiteetin käsitteeseen. Ydinidentiteetti tun-

netaan tyypillisesti englanninkielisillä nimillä PID (Personal Identifiable Data) [25] tai PII (Personal Identifiable Information) [26], joista tässä työssä käytetään termiä PID. Ydinidentiteetti käsittää henkilötiedot, joilla henkilö voidaan tunnistaa suoraan sekä tiedot, joilla henkilö voidaan tunnistaa epäsuoraan, eli kun se yhdistetään muun identiteetin määrittävän informaation kanssa [26]. Esimerkkeinä ensimmäisestä ryhmästä ovat nimi, sosiaaliturvatunnus, puhelinnumero ja sähköpostiosoite, sekä toisesta ryhmästä sukupuoli, etnisyys, syntymäpäivä ja asuinpaikka [26]. Ydinhenkilöllisyyttä voidaan pitää identiteetin määrittävän informaation arkaluontoisimpana osana, jonka perusteella henkilö voidaan helposti tunnistaa. Ydinhenkilöllisyyden sisältö saattaa vaihdella käytössä olevan vahvan sähköisen tunnistamisprotokollan määritelmän mukaisesti. Esim. SIOPv2-protokollan määritelmän dokumentaatiossa on taulukko, joka sisältää ydinhenkilöllisyyden eli PID:in kentät. Dokumentaatio on nähtävissä lähteessä [27]. Piiruntarkka ydinidentiteetin sisällön käsittely on epäolennaista, tärkeää on tietää, että PID koostuu arkaluontoisesta henkilötiedosta, jonka perusteella kohteet tyypillisesti tunnistetaan vahvoissa sähköisissä tunnistautumismenetelmissä.

## 2.2 Identiteetinhallinta

Identiteetinhallinnan tehtävänä on tarjota käytännöllinen menetelmä identiteetin määrittävän informaation hallintaan sekä identiteetin ylläpitoon [24]. Identiteetinhallinnan avulla ainutlaatuisille yksilöille luodaan ainutlaatuisia digitaalisia identiteettejä joita voidaan ohjata, päivittää ja valvoa koko identiteetin elinkaaren ajan [24]. Vaikka yksilöllä on vain yksi digitaalinen identiteetti, se voi sisältää useita digitaalisia tilejä, joissa kussakin on oma identiteetinhallintamekanismi [24]. Käytetty identiteetinhallintamekanismi suunnitellaan tyypillisesti tilin sisältämän tiedon laadun ja arkaluontoisuuden perusteella. Identiteetin käyttäjän, eli kohteen, näkökulmasta identiteetinhallinta käsittelee erityisesti valtuustietoa ja sen hallintaa.

Esimerkiksi Matti Meikäläinen voi käyttää työpaikan tarjoamaa toimikorttia henkilöllisyytensä todentamiseksi, mutta tiettyjen työtilanteen turvallisuusvaatimusten johdosta työnantaja, eli identiteetintarjoaja, voi päättää, että tunnistautuminen toimikortilla on pääsyoikeutena riittämätön. Päätös perustuisi identiteetinhallinnassa tapahtuneeseen toteamukseen, että toimikortin, ja sitä kautta toimikortin omistajan identiteetin, väärinkäytön riski on liian korkea [24]. Riski voidaan välttää tai eliminoida esimerkiksi edellyttämällä biometristen ominaisuuksien, kuten iirisskannerin, käyttöä tunnistautumisessa. Näiden laitteiden toimintavarmuus on erittäin korkea [20] ja niillä todennettavien fyysisten ominaisuuksien tarkastaminen vaatii Matti Meikäläisen fyysisen läsnäolon. Iirisskanneri ja toimikortti eivät myöskään sisällä, tunnista tai valtuuta yhtä ja samaa identiteettiä. Työpaikan toimikortti on kulkuavain, joka yhdistää kortin käyttäjän yrityksen kulunvalvonnasta löytyvään henkilöön kortin oikeutetusta käytöstä riippumatta [28]. Toimikortti ei välitä siitä, kuka korttia käyttää, se valtuuttaa kenet tahansa omistajansa digitaalisella identiteetillä [28]. Toimikortista poiketen iirisskanneri lukee käyttäjän iiriksen ja vertaa sitä muistissa olevaan iirikseen [29], eli valtuustietona toimii Matti Meikäläisen fyysinen identiteetti. Identiteetinhallinta on olemassa juuri sellaisia tilanteita varten, joissa identiteetin valtuustieto on joutunut vääriin käsiin. Jos Matti Meikäläisen toimikortti varastetaan, korttia voidaan käyttää vapaasti ja sen palauttaminen on kyseenalaista, eikä välittömästi estä identiteetin väärinkäyttöä. Ratkaisu rakentuu identiteetinhallintamenetelmään: menetetyn valtuustiedon mitätöinti. Kun työnantaja mitätöi Matti Meikäläisen toimikortin, oikeudeton käyttö päättyy välittömästi ja tilanne de-eskaloituu vaivattomasti. Vanhan toimikortin mitätöimisen jälkeen työnantaja myöntää Matille uuden toimikortin ja poikkeustilanne päättyy.

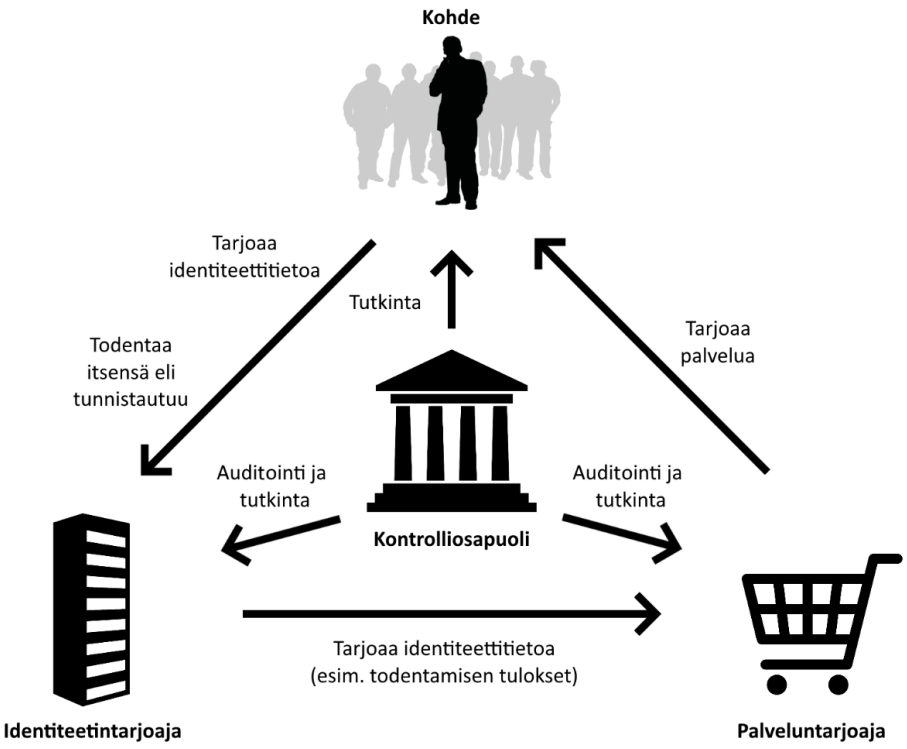
Myös identiteetin elinkaari ja identiteetinhallinnan osapuolet ovat osa identiteetinhallintaa. Elinkaari koostuu viidestä osasta [23, p. 29], joista ensimmäinen on provisiointi, eli identiteetin luonti. Provisioinnissa määritellään identiteetti sekä sen

sisältämä informaatio. Provisioinnin jälkeen identiteetti on olemassa ja käyttökelpoinen. Elinkaaren toinen lohko on käyttö, jolloin identiteetti on aktiivisessa käytössä. Elinkaaren kolmas lohko, päivittäminen, tapahtuu yhtäaikaisesti käytön kanssa. Identiteetin päivittämisellä varmistetaan, että identiteetin määrittävä informaatio vastaa todellisuutta. Erityisesti tunnisteet, kuten kotiosoite ja puhelinnumero, ovat muuttuvia ja ajan tasalla pidettäviä tietoja. Elinkaaren neljäs lohko on deprovisiointi, jossa identiteetti terminoidaan. Identiteetin käyttäminen ei ole mahdollista deprovisioinnin jälkeen. Elinkaaren viides ja viimeinen osa on hallinnointi, joka on koko elinkaaren ohella tapahtuva lohko. Identiteetin hallinnoinnissa organisaation identiteettipoliitikointi määrittelee missä, miten ja millä valtuuksilla identiteettiä voidaan käyttää [23, p. 36]. Hallinnoinnissa valvotaan identiteetin käyttöä ja vaatimustenmukaisuutta organisaation politiikkaa vastaan [23, p. 36]. Hallinnoinnissa määritellään millaisissa olosuhteissa kohde voi tunnistautua identiteettinsä avulla erilaisten palveluiden tai oikeuksien hyödyntämiseksi [23, p. 36]. Esimerkiksi eläkkeelle siirtyneen työntekijän pääsyöoikeus työpaikan iirisskannerissa voidaan terminoida organisaation politiikassa määritellyn toimintatavan perusteella. [23]

Identiteetinhallinnassa on neljä osapuolta, joista ensimmäinen on kohde. Kohde on henkilö, eläin, laite tai muu kohde, jota luotu identiteetti edustaa [23]. Esimerkiksi henkilöllisyystodistuksessa esitetty identiteetti edustaa omistajaansa. Identiteetinhallinnan toinen osapuoli on identiteetintarjoaja, joka myöntää ja hallinnoi kohteiden identiteettejä. Identiteetintarjoaja syöttää identiteetin määrittävän informaation, sitoo kohteen attribuutit muihin attribuutteihin mikäli niillä on yhteyksiä, luo vakuudet identiteetin oikeellisuudelle ja myöntää kohteelle valtuudet identiteetin käyttöön [23, p. 27]. Identiteetintarjoaja pystyy myös sitomaan myöntämiensä identiteettien attribuutteja toisten identiteetintarjoajien myöntämien identiteettien attribuutteihin. Esimerkiksi pankin toimesta myönnetty tilinumero voidaan sitoa valtion myöntämään sosiaaliturvatunnukseen [23, p. 27]. Identiteetinhallinnan kolmas

osapuoli on palveluntarjoaja, joka tarjoaa palvelun, jossa identiteettiä voidaan hyödyntää. Esimerkiksi useat verkkosivut tarjoavat palveluita rekisteröityneille käyttäjille käyttäjätunnusten myöntämiä valtuuksia vastaan [23, p. 27]. Neljäs ja viimeinen osapuoli on kontrolliosapuoli, joka koostuu tyypillisesti valtion valvontavirastoista ja säätelyelimistä. Yleisessä mittakaavassa kontrolliosapuolilla on tyypillisesti valtuudet päästä käsiksi identiteetintarjoajien tietopankkeihin, jotka koostuvat mm. identiteeteistä sekä rekistereistä, joita muodostetaan niiden käytön perusteella [23, p. 28], mutta käytännön järjestely riippuu valvottavasta teknologiasta. Kontrolliosapuoli toimii pääosin tutkinnallisissa ja valvonnallisissa tehtävissä [23, p. 28].

Identiteetinhallinnan osapuolien näennäisesti erilliset tehtävät eivät estä useamman osapuolen tehtävien hoitamista yhden ja saman henkilön tai tahon toimesta. Esimerkiksi internetissä luodun profiilin tapauksessa identiteetintarjoaja ja palveluntarjoaja voivat olla yksi ja sama taho: verkkosivusto, jolle kohteen identiteetti on luotu [23, p. 28]. Jos sivustolla on sivuston luoma admin-käyttäjä, kyseisen identiteetin kohde ja identiteetintarjoaja ovat yksi ja sama taho. Toinen esimerkki on tilanne, jossa kontrolliosapuoli ja identiteetintarjoaja ovat yksi ja sama järjestö. Tämä on mahdollista esimerkiksi silloin kun palveluntarjoaja käyttää Kela-tunnuksia palveluissaan, jolloin Kela on identiteetintarjoaja ja potentiaalisesti toimii identiteetinhallinnan kontrolliosapuolena. Osapuolien väliset suhteet esitellään kuvassa 2.2.




Kuva 2.2: Identiteetinhallinnan osapuolet [23, kuva 2.2, piirretty uudestaan]

## 2.3 Fyysisen ja digitaalisen identiteetin yhteenveto

Identiteetti kuvailee kohdetta fyysisessä ja/tai digitaalisessa järjestelmässä. Se koostuu identiteetin määrittävästä informaatiosta, joka jaetaan tunniste- ja valtuustietoihin sekä attribuutteihin. Kohteella on vain yksi fyysinen ja digitaalinen identiteetti, mutta digitaalinen identiteetti voi sisältää tilejä useiden organisaatioiden sisällä. Identiteetti sisältää kohteen luontaisia ominaisuuksia sekä muiden tahojen kanssa sovittuja ominaisuuksia. Identiteetin määrittävä informaatio voidaan jakaa kolmeen luotettavuustasoon tiedon luonteen perusteella.

Identiteettien käsittelyä ja hallintaa kutsutaan identiteetinhallinnaksi. Identiteetinhallinnassa on neljä osapuolta, joista kullakin on keskeinen rooli. Neljä osapuolta

ovat kohde, identiteetintarjoaja, palveluntarjoaja ja kontrolliosapuoli. Yksi henkilö/taho voi toimia useampana osapuolena yhtäaikaisesti. Identiteetillä on elinkaari, joka koostuu viidestä vaiheesta: provisiointi, käyttö, päivittäminen, deprovisiointi ja hallinnointi.

# 3 Sähköisen tunnistautumisen tarve ja käyttö

Suomen valtio, samoin Euroopan Unioni [30], on ottanut aktiivisen roolin valtion sähköisten toimintojen kehittämisessä. Näihin eurooppalaisiin sähköisiin palveluihin tunnistautuminen tulee tapahtumaan digitaalisen identiteetin avulla, nostattaen sähköisten identiteetintarjoajien ja palveluntarjoajen markkina-asemaa. Julkisen sektorin, kuten valtion virastojen, sähköisten palveluiden ja vahvan sähköisen tunnistautumisen tarjonta tulee muuttumaan vaatimukseksi tällä kehityksen tiellä. Todellisuudessa sähköiset palvelut ovat elintärkeitä jo nykypäivänä, sillä mm. verkkokauppojen ja tilauspohjaisten palveluiden kasvava suosio kasvattaa niiden aktiivista käyttäjämäärää kaikkialla maapallolla. Vuonna 2019 suomen valtion sähköisiä tunnistautumismenetelmiä hyödynnettiin noin 110 miljoonaa kertaa ja arvioitu laajentuminen vuodelle 2020 ulottui 140 miljoonaan tunnistautumiseen. Kasvavan suosion ja tarpeen vuoksi sähköisten tunnistautumismenetelmien tulisi olla kaikkien saatavilla. Suomessa tähän tarpeeseen vastaa Digi- ja väestötietovirasto eli DVV, jonka vuonna 2020 lanseeraama Digital identity program pyrkii tarjoamaan digitaaliseen identiteettiin perustuvan sähköisen tunnistautumismenetelmän kaikille suomalaisille. Järjestelmä tulisi toimimaan ilmaisen ja helppokäyttöisen puhelinsovelluksen muodossa [30]. [31]

Kansallisella tasolla digitaalisen henkilöllisyyden, ja myöhemmin identiteettilom-

pakon, implementaatio on suunniteltu asettumaan nykyisten suomalaisten sähköisten tunnistautumismenetelmien rinnalle, jolloin sähköisen palvelun käyttäjä voi valita haluamansa tunnistautumismenetelmän. Järjestelmän on tarkoitus olla kaikenkattava, jotta uuden järjestelmän toimivuus ei olisi yhtä rajoittunutta kuin nykyisten. Nykyisten tunnistautumismenetelmien ongelmana on se, että sähköisten palveluiden tarjoajien täytyy erillisesti tukea kutakin tunnistautumismenetelmää, eli nykyisten järjestelmien toimivuus rajoittuu niitä tukeviin pisteisiin. Esimerkiksi Osuuspankin sähköistä pankkitunnistautumista voidaan hyödyntää ainoastaan asiointipalveluissa, jotka tukevat kyseistä tunnistautumismenetelmää [32]. Digitaalinen henkilöllisyys sen sijaan mahdollistaa toteutuessaan sähköisen tunnistautumisen kaikkiin julkisiin paikkoihin ja palveluihin vähintään Suomen mantereella. Kiteytettynä eurooppalaisen digitaalisen henkilöllisyyden ja identiteettilompakon tavoitteena on tarjota yksi suuri jäsenvaltioiden tukema ja ylläpitämä digitaalinen tunnistautumismenetelmä nykyaikaisten yksityisten tunnistautumisjärjestelmien paikalle. Kun valtiollinen tunnistautumismenetelmä tulee vaihtoehdoksi markkinoille, yksityiset ja rinnakkaiset järjestelmät joutuvat luopumaan nykyisestä valta-asemastaan. Ymmärtääkseen tämän muutoksen merkityksen, täytyy näiden järjestelmien nykytilanne ymmärtää yksityiskohtaisesti. [31] [30]

Suomessa on tällä hetkellä neljätoista kansallista eID-identiteetintarjoajaa (eID = elektroninen identifikaatio [33]), joista kolmetoista on yksityisen sektorin kehittämiä ja ylläpitämiä. Näistä kymmenen järjestelmää kuuluu Suomessa toimiville pankeille ja kolme on matkapuhelinoperaattorien lanseeraamia järjestelmiä. Neljästoista järjestelmä on ainoa julkisen hallinnon tarjoama eID-järjestelmä Suomessa, ja se on Digi- ja väestötietoviraston ylläpitämä. Näistä neljästätoista järjestelmästä pankkien lanseeraamat järjestelmät ovat käytetyimpiä ja niitä hyödynnetäänkin yksityisten sekä julkisten palveluiden lähes standardinmukaisena vahvana sähköisenä tunnistautumismenetelmänä. Näitä tunnistautumismenetelmiä käytettäessä käyttä-

jä, eli kohde, kirjautuu palveluun omilla pankkitunnuksillaan, jotka ovat kohteen digitaaliseen identiteettiin sidottua valtuustietoa. [31]

Käytännönläheisestä näkökulmasta katsottuna tunnistautuminen kyseisillä menetelmillä tapahtuu seuraavasti. Kun palveluntarjoajan sivusto vaatii vahvan sähköisen tunnistautumisen, se voi ohjata käyttäjän selaimen tunnistautumiseen. Tyypillisesti käyttäjälle aukeaa mahdollisuus valita haluamansa tunnistautumismenetelmä. Tunnistautumismenetelmän valinta ohjaa käyttäjän identiteetintarjoajan tunnistautumispalveluun, jossa käyttäjä esittää valtuustietonsa ja onnistuneen tunnistautumisen jälkeen identiteetintarjoajan sivusto ohjaa käyttäjän takaisin palveluntarjoajan sivustoon [34]. Esimerkiksi Kelan kotisivulle tunnistautuminen noudattaa tätä kaavaa [34]. Operaatio kirjaudu -> henkilöasiakkaat välittää pyynnön tunnistautuminen.suomi.fi-sivustolle, joka kerää useamman sähköisen tunnistautumismenetelmän tarjoajan sivulle, josta käyttäjä valitsee haluamansa vaihtoehdon [34]. Suomi.fi-palvelu toimii siis välittäjänä, jolle Kela on ulkoistanut sähköiset tunnistautumispalvelunsa. Menetelmän valittuaan käyttäjä tunnistautuu identiteetintarjoajan sivustolla, jolloin identiteetintarjoaja palauttaa käyttäjän ydinidentiteetin (PID:in) Suomi.fi:hin ja Suomi.fi ohjaa sen Kelan asiointipalveluun [35]. Käyttäjä ohjataan takaisin Kelaan onnistuneen tunnistautumisen yhteydessä [34]. Jos palveluntarjoaja ja identiteetintarjoaja ovat yksi ja sama taho, käyttäjä voi pysyä samassa sivustossa tunnistautumisen alusta loppuun. Näin voi tapahtua esimerkiksi silloin, kun käyttäjä kirjautuu sisään omaan verkkopankkiinsa [32]. [31]

eID-tunnistautumismenetelmien kansallinen lainsäädäntö perustuu Euroopan unionin määrittelemään eIDAS-säännöstöön [33]. eIDAS (lyhenne sanoista electronic Identification, Authentication and Trust Services) määrittelee yhtenäiset puitteet turvalliselle, nopealle ja tehokkaalle sähköiselle vuorovaikutukselle kaikissa EU-maissa [33]. eIDAS-säännöstössä määritellään kolme sähköisen tunnistautumisen turvallisuustasoa: eIDAS Low, eIDAS Substantial ja eIDAS High [36]. Suomessa käytös-

sä olevista neljästätoista järjestelmästä valtaosa on rekisteröity tasolle Substantial [37]. DVV:n digitaalinen varmenne on rekisteröity korkeammalle eIDAS High-tasolle [37]. eIDAS Low-tason tunnistautuminen ei ole kelvollinen turvallisuustaso vahvalle sähköiselle tunnistautumiselle, sillä se määritellään itserekisteröitymisenä [36]. Esim. sähköpostin alatunniste ja skannattu käsinkirjoitettu allekirjoitus ovat kelvollisia eIDAS Low-tason tunnisteita, koska niiden oikeellisuus on sidottu lähettäjän rehellisyyteen eivätkä ne välttämättä sisällä metatietoja kuten tunnistautumisen päivämäärää tai kellonaikaa [38]. eIDAS Low-tasoa käytettäessä tunnisteen vastaanottaja ei pysty todistamaan, että lähettäjän kanssa solmitut sopimukset on tehty kohteen suostumuksella [38]. eIDAS Substantial-tason sähköisen tunnistautumisen tulee täyttää seuraavat eIDAS-säännöstön artiklassa 26 määritellyt edellytykset: [38]

1. Allekirjoituksella on ainutlaatuinen yhteys allekirjoittajaan.
2. Allekirjoittaja voidaan tunnistaa sähköisen allekirjoituksen perusteella.
3. Voidaan vahvasti luottaa siihen, että allekirjoitus on tuotettu tiedolla jota ainoastaan allekirjoittaja hallitsee.
4. Allekirjoitus linkitetään sillä allekirjoitettuun tietoon siten, että tiedon muutokset ovat havaittavissa.

eIDAS Low-tasolla näitä vaatimuksia ei ole, siksi se ei ole riittävä turvallisuustaso kahden toisiaan tuntemattoman tahon vahvassa sähköisessä tunnistautumisessa [38]. eIDAS High-taso lisää vielä kaksi allekirjoituksen tuottajaan ja sertifiointiin liittyvää vaatimusta, jotka tekevät tämän turvallisuustason sähköisestä tunnistautumisesta laillisesti yhtä pätevän kirjallisen allekirjoituksen kanssa [38]. Rakenteellisesti tunnistautumisprosessi ei muutu Substantial- ja High-tasojen välillä. [31]

## 3.1 Finnish Trust Network (FTN)

Sähköisten tunnistautumisjärjestelmien täytyy noudattaa lain- ja standardienmukaisia vaatimuksia, joten järjestelmien käyttöönoton hallinta ja niiden toiminnan aktiivinen valvonta ovat elintärkeässä roolissa vastuullisen ja luotettavan tunnistautumisen mahdollistamiseksi. Suomessa eID-järjestelmien valvonnasta vastaa Liikenne- ja viestintävirasto Traficom, jonka toimintaelimenä toimii Kyberturvallisuuskeskus [31]. Jokaisen suomeen sijoittuneen eID-palveluntarjoajan täytyy lähettää kirjallinen ilmoitus Kyberturvallisuuskeskukseen ennen järjestelmän käyttöönottoa [31], jonka yhteydessä palveluntarjoaja antaa Traficomille oikeuden monitoroida palvelun lainsekä säädöstenmukaisuutta [31]. Kyberturvallisuuskeskuksen hyväksymät ja valvomat eID-palvelut muodostavat luottamusverkoston, joka on nimeltään Finnish Trust Network (FTN) [31]. Verkosto on ollut käytössä 01.05.2017 alkaen [31]. Se on kokoelma valtion toimielimen hyväksymiä ja valvomia digitaalisia tunnistautumispalveluntarjoajia. Luottamusverkosto muodostaa kokonaisuuden, jonka avulla turvallinen ja yhtenäinen sähköinen tunnistautuminen voidaan tarjota erilaisille sovelluksille ja asiointipalveluille yksittäisen sopimuksen perusteella [39]. Palvelunomaisessa järjestelyssä asiointipalvelu tarvitsee sähköisen tunnistautumisen ja FTN tarjoaa keskitetyn, turvallisen ja aktiivisesti valvonnanalaisen kokoelman tunnistautumispalveluita, jotka mahdollistavat vahvan sähköisen tunnistautumisen asiointipalveluun palveluntarjoajan puolesta [39]. Tällä menettelyllä asiointipalvelun tarjoajan ei tarvitse sopia erillisiä sopimuksia kaikkien verkostoon kuuluvien tunnistautumispalveluiden kanssa [39], mikä helpottaa vahvan sähköisen tunnistautumisen omaksumista eri palveluiden välillä [31]. Liikenne- ja viestintävirasto päättää myös luottamusverkoston palveluiden lainmukaisesta hinnoittelusta [31]. Liikenne- ja viestintävirasto ylläpitää rekisteriä kaikista suomeen sijoittuneista vahvan sähköisen tunnistautumisen tarjoajista. Rekisteri on julkisesti saatavilla Liikenne- ja viestintäviraston kotisivuilla [37]. FTN:n yhden sopimuksen menettely on edesauttanut sähköisen tunnistautumisen

yleistymistä suomalaisissa palveluissa [40]. [41]

Myös loppukäyttäjän näkökulmasta järjestelmän hyödyt ovat selkeitä. Esimerkiksi kappaleessa 3 esitetty esimerkki Kelaan tunnistautumisesta toimii FTN:n avulla [40]. Kela hyödyntää Suomi.fi-e-identifikaatiota palveluissaan [34]. Suomi.fi-palvelu ja FTN ovat suorassa yhteydessä toisiinsa, sillä Suomi.fi valjastaa FTN:ään rekisteröidyt palveluntarjoajat julkisen sektorin käyttöön [31]. Suomi.fi ja FTN toimivat nykyään yhteistyössä siksi, että Suomi.fi on FTN:n suora edeltäjä [40]. Suomi.fi-palvelun ansiosta Kela pystyy tarjoamaan luotettavan ja turvallisen vahvan sähköisen tunnistautumisen kaikille asiakkailleen solmimatta erillisiä sopimuksia eri tunnistautumispalveluiden kanssa [41]. Koska Kela hyödyntää FTN-palvelua, asiakas voi kirjautuessaan valita haluamansa tunnistautumismenetelmän annettujen vaihtoehtojen väliltä [34]. Verkosto parantaa vahvan sähköisen tunnistautumisen tarjontaa ja yhtenäisyyttä eri asiointipalveluiden välillä [41], edistäen loppukäyttäjien kykyä hyödyntää sitä [40]. Vuonna 2018 Suomi.fi mahdollisti n. 87 miljoonaa, vuonna 2019 n. 110 miljoonaa [40], vuonna 2020 n. 155 miljoonaa ja vuonna 2021 melkein 200 miljoonaa sähköistä tunnistautumista [42]. Tilastojen perusteella kokonaistunnistusmäärä voi ylittää 250 miljoonan rajan vuonna 2022 [42]. On huomattava, että FTN:n olemassaolo on yhtenäistänyt sähköisen tunnistautumisen hinnoittelua eri palveluntarjoajien välillä, laskenut tunnistautumisen hinnastoa yleisesti, parantanut elektronisen tunnistautumisen saatavuutta, helppokäyttöisyyttä ja kilpailutusta sekä parantanut vahvan sähköisen tunnistautumisen luotettavuutta [40].

### 3.1.1 FTN:n ongelmat

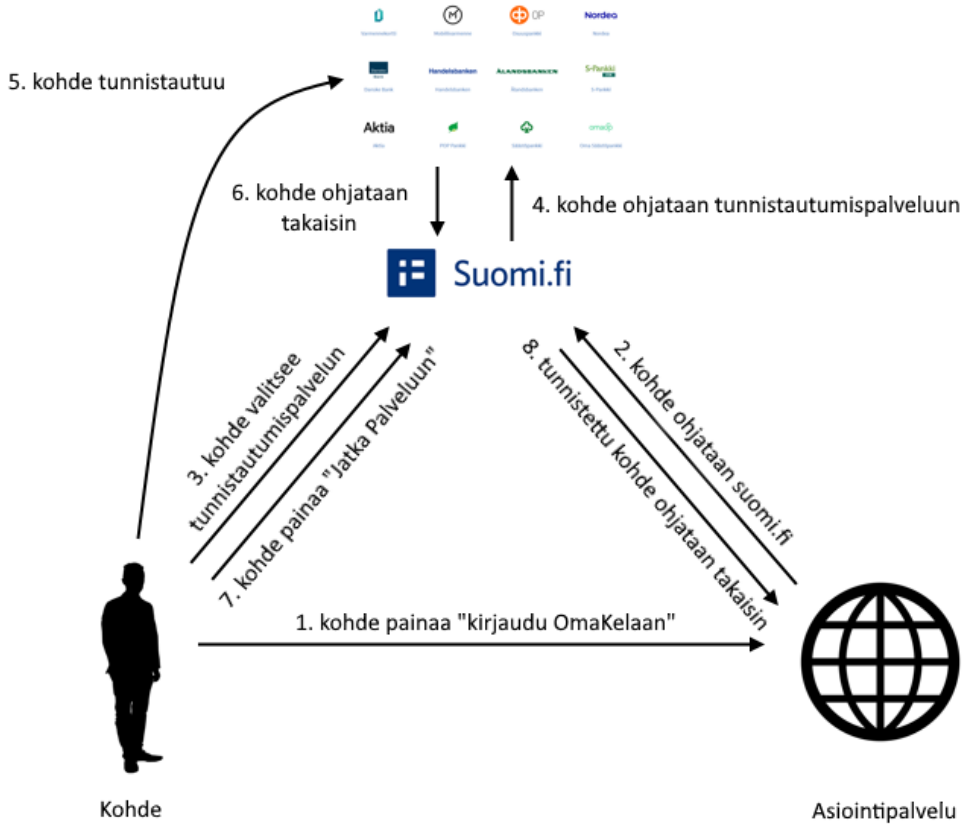
Huomattavista eduistaan huolimatta FTN ei ole puutteeton ratkaisu. FTN:n kaksi suurinta ongelmaa ovat tunnistautumismaksu, jonka FTN:ään kuuluvat yksityiset tunnistautumismenetelmäntarjoajat perivät jokaisesta tunnistautumisesta [43], sekä epäsuora luottamussuhde DVV:n ja loppukäyttäjän välillä [39]. Asiointipalvelu,

esimerkiksi DVV, joutuu maksamaan jokaisesta tunnistautumisesta, joka tapahtuu yksityisen tarjoajan toimesta FTN:n välityksellä [43] [39]. Epäsuoralla luottamussuhteella viitataan siihen, että loppukäyttäjä asettaa luottamuksensa tunnistautumismenetelmien verkostoon, jota Traficom hallitsee, ei suoraan Traficomiin [39]. Yksityisten toimijoiden tuottama välikerros toimii välikappaleena, joka rikkoo muutoin suoran luottamussuhteen loppukäyttäjän ja palveluntarjoajan välillä [39]. Näistä puutteista huolimatta FTN:ää voidaan pitää toimivana ja turvallisena ratkaisuna digitaaliseen tunnistautumiseen. Käyttäjäkokemusta silmällä pitäen järjestelmässä on myös rakenteellinen haaste: sähköinen tunnistautuminen vaatii siirtymisen ulkoiseen tunnistautumispalveluun, josta käyttäjä siirretään takaisin asiointipalveluun [34]. Tunnistautuminen ei ole saumatonta ja siinä on monta etappia, eikä asiointipalvelu voi vaikuttaa käyttäjäkokemukseen tunnistautumisen aikana, sillä se tapahtuu ulkoisen tahon toimesta. Esim. Kela-esimerkissä Kela (asiointipalvelu) ei ole vastuussa Suomi.fi-palvelun käyttäjäkokemuksesta [34]. Koska Kela hyödyntää FTN:n palveluita, loppukäyttäjä ei voi tunnistautua siirtymättä ulkoiseen tunnistautumiseen. Tällöin käyttäjän tehtävä "Tunnistautuminen"muuttuu seuraavaksi pienempien tehtävien sarjaksi [34]:

1. Käyttäjä painaa painiketta "Kirjaudu OmaKelaan".
2. (Automaattinen) Selain ohjautuu sivustolle tunnistautuminen.suomi.fi.
3. Käyttäjä painaa haluamansa tunnistautumispalvelun kuvaketta.
4. (Automaattinen) Käyttäjä ohjataan tunnistautumispalveluun.
5. Käyttäjä tunnistautuu tunnistautumispalveluun omilla käyttäjätunnuksillaan, mobiiliavaimella tai muulla mekanismilla.
6. (Automaattinen) Käyttäjä ohjataan takaisin tunnistautuminen.suomi.fi-palveluun.

7. Käyttäjä valitsee "Jatka Palveluun".

8. (Automaattinen) Tunnistettu käyttäjä ohjataan takaisin asiointipalveluun.




Kuva 3.1: FTN tunnistaa kohteen [34] [39]

Tätä prosessia ei voi pitää kovin sujuvana tai suoraviivaisena etenkään silloin, kun loppukäyttäjällä on hidas internet-yhteys. Viisikymmentä prosenttia etapeista tunnistautumattoman ja tunnistautuneen käyttäjän välillä tapahtuu automaattisesti, kun käyttäjän selainta ohjataan automaattisesti palvelusta toiseen. Jokainen uudelleenohjaus vie aikaa ja kaistanleveyttä. FTN:n rakenne paisuttaa tunnistautumisprosessia, eli rakennetta muuttamalla tunnistautuminen voi muuttua suoraviivaisemmaksi. Tästä esimerkkinä toimii tunnistautuminen asiointipalvelussa, joka on rekisteröitynyt FTN:n tunnistautumispalveluntarjoajaksi, kuten Nordean tai Osuus-

pankin kotisivussa [32]. Tunnistautuminen Osuuspankin asiointipalveluun mobiiliavaimella tapahtuu seuraavasti:

1. Käyttäjä painaa painiketta "Kirjaudu sisään".
2. (Automaattinen) Avautuu sivunäkymä, joka pyytää asiakkaan käyttäjätunnuksen.
3. Käyttäjä syöttää käyttäjätunnuksen ja painaa "Jatka".
4. Käyttäjä avaa mobiilisovelluksen puhelimessaan asiointipalvelun kehotuksesta ja vahvistaa tunnistamisen mobiiliavaimella.
5. (Automaattinen) Tunnistettu käyttäjä ohjataan asiointipalveluun.


Kuva 3.2: Osuuspankki tunnistaa kohteen mobiilisovelluksen avulla [32]

Koska Osuuspankki on yhtäaikaisesti sekä asiointipalvelu että tunnistautumispalvelu, selaimen ei koskaan tarvitse ohjata käyttäjää sivustolta toiselle kuten FTN-järjestelmässä täytyy. Selain uudelleenohjataan ainoastaan yhden kerran kun tunnistautuminen Osuuspankin etusivulla on valmis ja käyttäjä ohjataan asiointipalveluun. Tunnistautumispalvelun valintaa ei ole, koska ainoa Osuuspankin kotisivuilla tarjottu tunnistautumismenetelmä on Osuuspankki itse, ja käyttäjä ohjataan asiointipalveluun ilman käyttäjän erillistä hyväksyntää. Myös etappi kaksi, jossa sivunäkymä avautuu, voidaan suorittaa ns. "nolla-ajassa", eli kyseinen automaattinen etappi valmistuu ennen kuin käyttäjä on valmiina suorittamaan etapin kolme. Jos käyttäjän ei tarvitse odottaa tätä automaattista etappia, se ei kuluta käyttäjän aikaa, eikä täten haittaa hänen käyttäjäkokemustaan. Osuuspankin kotisivujen esittämässä tunnistautumisessa on ainoastaan tarpeellisia, eikä ollenkaan turhia etappeja, sillä määritelmänsä perusteella kohteen tunnistautuminen koostuu vain kolmesta etapista:

1. Identiteetintarjoaja pyytää digitaalisen identiteetin määrittelevän informaation.

2. Kohde luovuttaa identiteetin määrittelevän informaation.

3. Tunnistettu kohde ohjataan eteenpäin.

Kun tätä kolmen etapin prosessia verrataan Osuuspankin kotisivujen toimintaan, ensimmäinen eroavuus tapahtuu, kun käyttäjä ilmaisee, että hän haluaa tunnistautua painamalla "Kirjaudu sisään". Tämä on välttämätön etappi, sillä muutoin Osuuspankin kotisivuja ei voisi selata tunnistautumatta tai palvelun täytyy pyytää käyttäjää kirjautumaan, joka voi vahingoittaa sivuston käyttäjäkokemusta. Toinen ero on se, että käyttäjä myöntää kolme identiteetin määrittelevää informaatiota kahdesta eri paikasta. Käyttäjätunnus on tieto, joka kohteen tulee tietää [44]. Mobiiliavain on asia, joka kohteella tulee olla [44]. Mobiiliavaimen PIN-koodi on toinen tieto,

joka kohteen tulee tietää. Useamman identiteetin määrittelevän informaation pyytäminen tunnistautumisprosessissa tekee tunnistautumisesta vaativampaa, mutta lisää palvelun turvallisuutta tasoittain [44]. Tästä syystä useampien (tai korkeampien turvallisuustasojen) informaation pyytäminen käyttäjältä on oikeutettua vaikka se toimisi käyttäjäkokemuksen esteenä. Sopiva turvallisuustaso määritellään kontekstin perusteella.

Kuten näistä esimerkkitapauksista nähdään, Finnish Trust Networkin mukainen tunnistautuminen ei ole paras mahdollinen tunnistautumismenetelmä, kun tavoitteena on positiivinen käyttäjäkokemus. FTN:n suunnittelu pohjatasolta alkaen paisuttaa tunnistautumisen kestoa ja siihen tarvittavien etappien määrää, jolloin tunnistautuminen ei ole mahdollisimman suoraviivaista tai sujuvaa. Tästä ongelmasta huolimatta FTN:n hyödyt ovat huomattavasti suurempia kuin sen tuottamat haitat, eli järjestelmällä on hyvä hyöty/haittasuhde.

### 3.1.2 Vahvan sähköisen tunnistautumisen atomisaatio

Atomisaatio on termi, jota tyypillisesti käytetään kemiallisissa [45] ja yhteiskunnallisissa piireissä [46]. Atomisaatio on prosessi, jossa kiinteän tai nestemäisen aineen muodostavat atomit erkanevat toisistaan ja vapautuvat ympäröivään ilmaan [45]. Termi "atomisaatio"muodostuu siitä, että jaettavista kappaleista koostuva aine jakautuu pienemmiksi kappaleiksi, jotka ovat jakamattomia. "Atomi"tulee kreikan sanasta *atomos*, jonka suomenkielinen käännös on "jakamaton"[46]. Atomisoitunut kappale on siis jakamaton kappale. Yhteiskunnasta puhuttaessa atomilla tarkoitetaan yksittäistä ihmistä tai henkilöä, koska ihminen on yhteiskunnan jakamaton kappale [46]. Yhteiskunnan atomisaatiolla viitataan siihen, että yksinasuminen lisääntyy ja ihmisten syrjäytyminen lisääntyy, eli yhteiskunnan muodostavat ihmiset erkaantuvat omiin oloihinsa, eivätkä toimi yhteisössä [46]. Yhteiskunta jakaantuu kappaleisiin, joita ei ole mahdollista jakaa pienempiin kappaleisiin, eli atomisoituu

[46]. Esimerkiksi keilaaminen on peli, jota voi pelata yksin tai ryhmässä. Atomisoituneen yhteiskunnan jäsenet keilaavat yksin, yhteisöllisen yhteiskunnan jäsenet keilaavat ryhmässä [46].

Vahvan tunnistautumisen nykytilanne heijastaa tätä atomisaation määritelmää, sekä erityisesti sen perustana olevaa filosofiaa. Finnish Trust Network koostuu yksityisten toimijoiden kehittämistä tunnistautumispalveluista, jotka FTN niputtaa ja tarjoaa asiointipalveluille pääsyn kuhunkin luottamusverkon palveluun yhden sopimuksen välityksellä [39]. FTN-palvelu voidaan jakaa näihin yksityisiin tunnistautumispalveluihin, mutta jakaminen ei ole mahdollista tästä eteenpäin. FTN siis lieventää alan atomisaatioita kytkemällä atomisoituneet tunnistautumismenetelmät yhteen polkuun [39]. Yksi FTN:n vertailukohteista maapallolla on Niili, jolla on suora yhteys kaikkeen sen varsilla olevaan asutukseen, vaikkei asutuksella muutoin olisi suoraa yhteyttä toisiinsa. Niili on verkosto, joka niputtaa atomisoituneen asutuksen yhteen reittiin FTN:n tavoin [47] [40]. On selvää, että vahvan sähköisen tunnistautumisen tilanne nykypäivänä on atomisoitunut. FTN:n olemassaolo osoittaa, miksi atomisoitunut, yksittäisten kaupallisten toimijoiden muodostama ratkaisu ei ole hyvä ratkaisu valtakunnalliseen sähköiseen tunnistautumiseen. FTN:n valjastamana eID-teknologian valtakunnallisesta adoptiosta on tullut helpompaa sekä asiakaspalveluille että palveluiden käyttäjille, asiakaspalveluiden maksama hinta tunnistautumispalveluille on laskenut ja yhtenäistynyt, tunnistautumismenetelmien valvonta, turvallisuus ja luotettavuus ovat kasvaneet ja tunnistautumista vaativien palveluiden sähköisestä käytöstä on tullut tavanomaista [40]. Ilman FTN:ää yksikään näistä positiivisista muutoksista ei välttämättä olisi tapahtunut muutoin kuin organisaatioiden välisen kilpailun [48] tai vahvaa sähköistä tunnistautumista koskevan lainsäädännön mahdollistamana. Atomisoituneessa järjestelmässä käyttäjän täytyy luoda erillisiä tunnuksia erillisiin organisaatioihin niiden erillisen federoinnin vuoksi, luottaa kuhunkin niistä erikseen ja kohdata tilanteita, joissa aiemmin käyttämättömän tunnis-

tautumismenetelmän käyttöönotto on vaatimus uudella sivustolla. FTN:n ansiosta vahva sähköinen tunnistautuminen kaikkialle yhdellä tunnistautumismenetelmällä on yleensä mahdollista [39], mutta luottamussuhde käyttäjän ja Traficomin välillä on kuitenkin epäsuora yksityisen tunnistautumismenetelmän tuottaman välikerroksen seurauksena [40]. Seuraavan sukupolven sähköinen tunnistautuminen tuleekin todennäköisesti perustumaan yhteen valtion hyväksymään ja ylläpitämään tunnistautumismenetelmään, jolla voidaan korjata esitetyt FTN-järjestelmälle luontaiset ongelmat [31].

## 3.2 Nykyaikaisen sähköisen tunnistautumisen yhteenveto

Liikenne- ja viestintävirasto Traficom ylläpitää vahvojen sähköisten tunnistautumismenetelmien rekisteriä suomessa. Sähköisen tunnistautumisen suosio on ollut jatkuvassa kasvussa viime vuosina ja sen tarjoaminen asiakkaille on erittäin tärkeää. Sähköisten palveluiden ja -tunnistautumisen tarjoaminen voidaan nähdä jopa vaatimuksena. Suomessa on tällä hetkellä neljätoista kansallista eID-identiteetintarjoajaa, joista kymmenen kuuluu pankeille, jotka ylläpitävät lähes standardinomaista markkina-asemaa. Vahva sähköinen tunnistautuminen perustuu Euroopan unionin eIDAS-säännöstöön, jossa tunnistautumismenetelmät jaotellaan tasoihin eIDAS Low, eIDAS Substantial ja eIDAS High. Vahvat sähköiset tunnistautumismenetelmät asettuvat tyypillisesti tasolle eIDAS Substantial. eIDAS Low-taso kattaa ainoastaan itsetunnistautumisen, joten se ei kelpaa vastapuolen tunnistamiseen.

eID-järjestelmien toiminnasta ja valvonnasta suomessa vastaa Liikenne- ja viestintävirasto Traficom. Suomeen sijoittuneiden eID-palveluntarjoajien täytyy ilmoittaa kirjallisesti Traficomin Kyberturvallisuuskeskukseen ennen palvelun käyttöönottoa, jossa Traficomille myönnetään oikeus sen lain- sekä säädöstenmukaisuuden

valvontaan. Traficom on muodostanut luotettujen eID-palveluiden verkoston, joka nimettiin Finnish Trust Networkiksi (FTN) 01.05.2017. FTN niputtaa luotetut yksityiset tunnistautumismenetelmät yhteen siten, että asiointipalvelu voi hyödyntää niistä jokaista yhden sopimuksen perusteella. FTN on nopeuttanut vahvan sähköisen tunnistautumisen omaksumista ja yhtenäistänyt siitä koituvia palvelumaksuja. FTN:n ansiosta loppukäyttäjälle voidaan helposti tarjota luotettava ja turvallinen standardinmukainen vahvojen sähköisten tunnistautumismenetelmien kokoelma.

Positiivisista puolistaan huolimatta FTN ei ole täydellinen ratkaisu. Sen neljä suurinta ongelmaa ovat seuraavat:

1. Jokaisesta tunnistautumisesta peritään tunnistautumismaksu.
2. Yksityisten tunnistautumispalveluntarjoajien kerros estää suoran luottamussuhteen muodostumisen loppukäyttäjän ja Traficomin välille.
3. FTN-järjestelmän rakenne paisuttaa tunnistautumisprosessia.
4. FTN lieventää, muttei eliminoi, sähköisen tunnistautumisen atomisaatiota.

Seuraavan sukupolven sähköisen tunnistautumisen on tarkoitus välttää tai eliminoida nämä ongelmat. Suomessa tästä tulevasta ratkaisusta vastaa Digi- ja väestötietovirasto (DVV).

# 4 Eurooppalainen identiteettilompakko

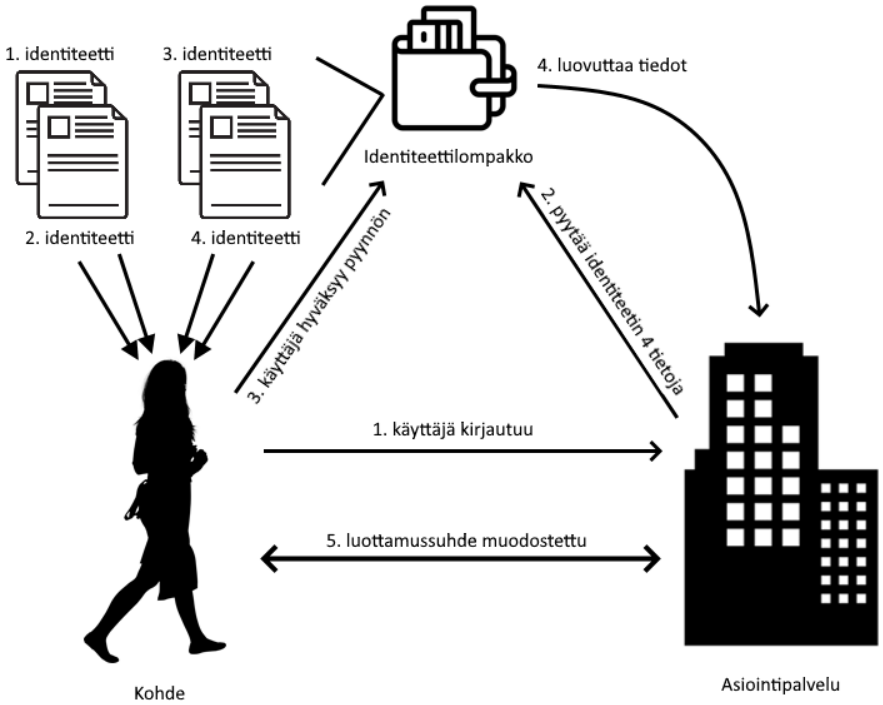
Kuten edellisen kappaleen lopussa todettiin, seuraavan sukupolven vahvan tunnistautumisen tulisi edistää alan kehitystä ulos atomisoituneesta rakenteesta, johon yksityisten toimijoiden tuottama ekosysteemi johtaa [30], koska kilpailevat yksityiset sektorin toimijat kehittävät kukin omia ja erillisiä vahvoja sähköisiä tunnistautumismenetelmiään asiakkaittensa käyttöön [31]. Näiden palveluiden käytöstä peritään tunnistautumismaksu jokaisen tunnistautumisen yhteydessä [43], kun tunnistautumismenetelmä implementoidaan asiointipalveluihin. Tämä tarkoittaa sitä, että jokainen tunnistautuminen esim. Kela.fi-palveluun [34], joka hyödyntää yksityisiä tunnistautumismenetelmiä kuten Osuuspankin tai Nordean vahvaa sähköistä tunnistautumista [39], tuottaa kustannuksen kyseiselle palveluntarjoajalle [43]. Palveluntarjoajilla on siis intressi uudenlaiselle tunnistautumisjärjestelmälle, jossa kustannukset ovat maltillisemmat. Vahvan sähköisen tunnistautumisen uuden sukupolven ideointi ja suunnittelu alkoi jo 2010-luvun loppupuolella [30], mutta sen varsinainen työstäminen Suomessa alkoi vasta vuonna 2020 Digi- ja väestötietoviraston lanseeraamana [31]. Projektin tarkoituksena on kehittää digitaalinen henkilöllisyys, jota hyödyntämällä EU:n kansalainen voi tunnistautua sähköisesti vahvaa tunnistautumista vaativiin palveluihin hyödyntämättä yksityisen sektorin tuottamia ratkaisuja, kuten pankkitunnuksia, ollenkaan [31]. DVV on julkaissut dokumen-

tin DVV/3873/2020, jossa esitetään, millä periaatteella uusi järjestelmä tulisi toimimaan ja millaisissa tilanteissa järjestelmää voitaisiin käyttää ja millä tavalla [31]. Dokumentin sisältöä esitetään tässä kappaleessa tarpeen mukaan. Dokumentin luonteen vuoksi projektin kuvaus on kuitenkin rajattu korkealle abstraktiotasolle [31]. Järjestelmän esittely makromittakaavassa on tarkoituksenmukaista; dokumentissa esitetään ainoastaan selvitys halutusta järjestelmästä ja sen toiminnoista, eikä siinä oteta kantaa toiminnallisen ratkaisun yksityiskohtiin [31]. Mikrotason ratkaisuista ja toiminnallisista yksityiskohdista vastaa tarjouspyyntöön vastaava yhteistyöyritys [31]. Uusi tunnistautumisjärjestelmä tulee hyödyntämään koko EU:n laajuista identiteettilompakon lainsäädäntökehikkoa, jota kansallisten hankkeiden tulee noudattaa [30]. Identiteettilompakon nimitystä voidaankin käyttää hyvin yhtenäisesti. [31, Ch. 4.3]

## 4.1 Identiteettilompakon aktivointi ja toiminta

Kirjoitushetkellä eurooppalaisen identiteettilompakon sovellutusta ei ole tuotu markkinoille, joten lompakon toiminnallisuuden selostukset perustuvat visioon. Korkean tason toiminnallisuusselosteista, kuten DVV/3873/2020-dokumentista [31] sekä Valtiovarainministeriön syksyllä 2021 järjestämästä VM Live-esityksestä [30] on mahdollista ymmärtää suurin piirtein, miten identiteettilompakko tulee toimimaan käytännössä. Aloittamalla kaikkein korkeimmalta mahdolliselta abstraktiotasolta eurooppalaisen identiteettilompakon koostumus voidaan jakaa käyttäjään, päätesovellukseen ja palveluntarjoajan taustapalveluun, jotka pystyvät kommunikoimaan keskenään [31]. Näistä ensimmäinen, eli käyttäjä, on kohde, joka käyttää eurooppalaista identiteettilompakkoa tunnistautumisvälineenä. Käyttäjä operoi päätesovellusta nykyaikaisen mobiililaitteen, tietokoneen tai verkkoselaimen välityksellä [30]. Päätesovellus on digitaalisen identiteettilompakon ydinkappale, joka tallennetaan käyttäjän päätelaitteeseen [30]. Päätesovellus käsittelee ja hallinnoi käyttäjän digitaalista iden-

titeettiä, siihen sisällytettyjä eri organisaatioihin kuuluvia tilejä, sen attribuutteja, sekä sen käyttöä [30]. Tunnistautumisprosessi alkaa käyttäjästä, joka pyrkii tunnistautumaan palveluntarjoajan asiointipalveluun. Asiointipalvelu pyytää käyttäjää tunnistautumaan identiteettilompakkoon tallennetulla identiteetillä. Käyttäjä avaa päätesovelluksen ja vastaa tunnistamispyyntöön, jolloin päätelaite lähettää vastauksen palveluntarjoajan taustapalveluun, joka tarkistaa pyynnön oikeellisuuden [31]. Tunnistautuminen päättyy, kun taustapalvelu hyväksyy tai hylkää tunnistautumisen [31]. Palveluntarjoajan taustapalvelu on siis kolmikon elementti, jonka tehtävänä on tarkistaa kohteen henkilöllisyys [31].




Kuva 4.1: Identiteettilompakolla tunnistautuminen [31] [30]

Käytännössä tältä abstraktiotasolta katsottuna eurooppalaisella identiteettilompakolla tunnistautuminen vaikuttaa täysin yhteneväiseltä nykyisiin tunnistautumismenetelmiin verrattuna, jotka myöskin koostuvat käyttäjästä, päätelaitteesta ja pal-

veluntarjoajan ylläpitämästä taustapalvelusta [32]. Eroja huomataan, kun identiteettilompakkoa ja sen toimintaa tarkastellaan tarkemmin. Eurooppalainen identiteettilompakko tulisi hallitsemaan useita, jopa kaikkia kohteen digitaaliseen identiteettiin kuuluvia tilejä, joilla voidaan osoittaa kohteen attribuutteja ja/tai oikeuksia sähköisessä asioinnissa [30]. Kuten nykyisissä tunnistautumismenetelmissä, eurooppalaiseen identiteettilompakkoon tarvitaan myös luotettavia identiteetintarjoajia näiden tilien luomista varten. Identiteetin tarjoamista voidaan tarkastella kenties tärkeimmän identiteettilompakoon kuuluvan tilin aktivoimisen kautta. Tili on henkilöllisyystodistusta vastaava digitaalinen henkilöllisyystodistus [30] [31]. Järjestelmän valtiollisen ja kansallisen tuen ansiosta identiteetintarjoajana toimii tässä tapauksessa valtion toimielin, esimerkiksi poliisilaitos, joka myöntää digitaalisen henkilöllisyystodistuksen kohteen perinteistä paperista henkilöllisyystodistusta vastaan. Kun kohde on saapunut poliisilaitokselle, laitoksen viranomainen pyytää kohteen henkilöllisyystodistusta, jotta hän voi varmistaa hakijan henkilöllisyyden valtion ylläpitämää väestötietojärjestelmää vastaan [31]. Onnistunutta tunnistautumista pidetään pätevänä perusteena myöntää paperista henkilöllisyystodistusta vastaava digitaalinen identiteetti kohteelle [31], joka tallennetaan kohteen eurooppalaiseen identiteettilompakkoon. Tämän prosessin jälkeen digitaalinen henkilöllisyystodistus on aktivoitu ja identiteettilompakon päätesovellus voi käyttää sitä sähköisessä tunnistautumisessa [30] [31]. Tätä identiteettilompakkoon tallennettua henkilöllisyystodistusta on tarkoitus pitää oikeudellisesti pätevänä digitaalisena versiona alkuperäisestä henkilöllisyystodistuksesta [30]. Aktivoidulla henkillöllisyystodistuksella höystettynä identiteettilompakkoa voidaan käyttää vahvana sähköisenä tunnistautumismenetelmänä, koska identiteetti on myönnetty virkamiehen toimesta henkilöllisyystodistusta ja valtion väestötietorekisteriä vastaan. Päätesovelluksen sisältämä hallinnointipaneeli antaisi käyttäjän hallita lompakkoon tallennettuja tilejä esim. kadonneiden tai varastettujen tilien sulkemista varten. Oletettavasti käyttäjä ei pystyisi muokkaa-

maan tilejä, koska se rikkoisi niiden rikkomattomuuden. Identiteettilompakko hyödyntää varmentajaa (certificate authority, CA) joka autentikoi kaikki lompakkoon kytketyt osapuolet. [31, Ch. 4.3]

On syytä huomata, että identiteettilompakon digitaalista henkilöllisyystodistusta ei välttämättä ole pakko aktivoida poliisilaitoksella, jos käyttäjällä on käytössä vahva tunnistautumismenetelmä kuten pankkitunnus tai valtion myöntämä henkilöllisyyskortti [6]. Syynä tähän on se, että kohde voi vahvistaa oman henkilöllisyytensä digitaalisesti näillä menetelmillä jo tänä päivänä. Itsenäinen rekisteröinti voi myös olla mahdollista tietynlaisten biometristen ominaisuuksien perusteella, kuten NFC:llä varustetun passin avulla, tai lainmukaisen huoltajan välityksellä esim. tapauksissa, joissa identiteetin kohde on vanhus tai lapsi. Tällä menetelmällä tilien aktivointi ja eurooppalaisen identiteettilompakon käyttöönotto onnistuisivat vaikka kohteen kotisohvalta, jolloin valtion resurssien tarve järjestelmän käyttöönoton yhteydessä voitaisiin minimoida. Identiteettilompakkoon tallennettu digitaalinen identiteetti voidaan purkaa DVV:n tai identiteetin omistajan toimesta esimerkiksi rikkeiden, identiteettivarkauden tai käyttäjän oman tahdon perusteella. Tunnistautuminen puretulla identiteetillä ei ole mahdollista, mutta sen uudelleenaktivointi tulisi olemaan mahdollista siten, että kohde ottaa yhteyden identiteetintarjoajaan ja todistaa henkilöllisyytensä uudelleen edellä mainittuja menetelmiä käyttämällä. Kuten identiteetin alkuperäisessä aktivointiprosessissa, uudelleenaktivoinnin tulee myös varmistaa, että myönnetty digitaalinen identiteetti vastaa oikeaa fyysistä identiteettiä reaalimaailmassa. [31, Ch. 4.3]

## 4.2 Identiteettilompakon edut

Identiteettilompakon tunnistautumiskapasiteetin tulisi alkaa siitä, että se mahdollistaa tunnistautumisen Suomi.fi-palvelun kautta [31]. Tällöin sivustoihin tunnistautuminen olisi mahdollista FTN-järjestelmän tai identiteettilompakon perusteella

[31] [34]. Eurooppalaisella identiteettilompakolla tehdyistä tunnistautumisista ei perittäisi tunnistautumismaksuja, FTN:llä tehdyistä perittäisiin [43] [31]. Eurooppalaisen identiteettilompakon mukaisessa Suomi.fi-tunnistautumisessa käyttäjä valitsee lompakkosovelluksella tunnistautumisen, jolloin välitetään tunnistautumispyyntö suoraan asiakkaan päätesovellukseen, jolloin tunnistautuminen voidaan suorittaa ainoastaan identiteettilompakkoa käyttämällä [30]. Ideaalitilanteessa Finnish Trust Networkin Suomi.fi:lle tarjoamat yksityiset tunnistautumismenetelmät voitaisiin korvata kokonaan identiteettilompakolla, jolloin tunnistautumisen atomisaatio-, maksullisuus- ja luottamussuhdeongelmat voitaisiin ratkaista perinpohjaisesti, mutta tällaista tulevaisuuden kehitystä voidaan pitää epävarmana. Käyttäjän näkökulmasta tunnistautuminen on helppoa. Kun käyttäjä yrittää kirjautua esim. Kela.fi-sivustoon, asiointipalvelu (Kela) lähettää tunnistautumispyynnön asiakkaan päätesovellukseen. Käyttäjä avaa päätesovelluksen tietokoneessa, mobiililaitteessa tai verkkoselaimessa ja avaa pyynnön, joka pyytää käyttäjän hyväksyntää. Käyttäjä autentikoi ja hyväksyy pyynnön esim. sovellukseen asetetulla PIN-koodilla ja tieto välittyy asiointipalvelun taustapalveluun, joka hyväksyy autentikaation sen oikeellisuuden tarkastamisen jälkeen. Tieto onnistuneesta autentikaatiosta välitetään Kela.fi-sivustolle [31, Ch. 4.4.1]. Eurooppalainen identiteettilompakko kykenee siis samantyyppisiin autentikointitehtäviin kuin esim. FTN nykypäivänä. Identiteettilompakko on julkinen palvelu, jonka saatavuus taataan kaikille ikä- ja ihmisryhmille yhdenvertaisuuden nimissä [30].

Vaikka digitaalinen henkilöllisyystodistus on yksi identiteettilompakon tärkeimmistä ominaisuuksista, sen tunnistautumiskapasiteetti ei rajoitu digitaaliseen versioon paperisesta henkilöllisystodistuksesta [30]. Identiteettilompakko on suunniteltu monikäyttöiseksi [30]. Identiteettilompakkoon voidaan tallentaa monia muitakin digitaalisia tilejä ja attribuutteja, jotka kohde voi esittää sähköisesti identiteettilompakon välityksellä [30]. Järjestelmää voidaan verrata todellisen maailman lom-

pakkoon, jossa mukana liikkuu huomattavasti enemmän kuin ajokortti tai henkilöllisyystodistus [30]. Esim. ajokortin, kela-kortin, opiskelijakortin ja kalastuskortin tiedot voidaan digitalisoida ja tallentaa eurooppalaiseen identiteettilompakkoon uusina digitaalisina tileinä, joiden perusteella kohde voi osoittaa mm. ajo-oikeuden ja opiskelijastatuksen olemassaolon mille tahansa sähköiselle palvelulle [30]. Myös kanta-asiakaskortit ja muut identiteettiin sidotut oikeudet on mahdollista liittää eurooppalaiseen identiteettilompakkoon [30]. Identiteettilompakon toiminnassa nähdään myös hyvin tärkeänä, että sovelluksen käyttäjän tarvitsee paljastaa itsestään ainoastaan välttämättömät tiedot tunnistautumisen yhteydessä [30]. Esim. täysikäisyys voidaan tarkistaa ilman nimen tai henkilötunnuksen luovuttamista toiselle osapuolelle [30], toisin kuin ajokorttia esitettäessä, jolloin kortin tarkastava virkamies pystyy lukemaan kaikki korttiin kirjoitetut tiedot. Tämä on perinteisten digitaalisten sekä fyysisten todentamismenetelmien heikkous, jossa esim. ajokortin tai henkilöllisyystodistuksen luovutuksen yhteydessä viranomainen voi lukea syntymäajan lisäksi myös kaiken muun informaation kuten kohteen nimen ja sosiaaliturvatunnuksen [6].

## 4.3 Identiteettilompakon perusta

Eurooppalainen identiteettilompakko perustuu kesäkuussa 2021 julkaistuun eIDAS-asetusehdotukseen, joka säätelee sähköistä tunnistautumista sekä sähköisen asioinnin luottamuspalveluita [30]. Kun lompakko otetaan käyttöön, lompakon sähköinen tunnistautuminen ja palvelut, joihin lompakolla tunnistaudutaan, noudattavat molemmat eIDAS-asetusta muiden sähköisten tunnistautumismenetelmien ohella [30]. Kesäkuussa 2021 annetut muutokset koskevat lompakkosovellusten lainsäädäntöä, yksityisen sektorin palveluissa asioimisen lainsäädäntöä ja sähköisen tunnistautumisen järjestelmien ilmoittamisen, eli notifioimisen, lainsäädäntöä. Ilmoittamisella tarkoitetaan sitä, että EU:n jäsenvaltioilla on tulevaisuudessa velvollisuus ilmoittaa

ainakin yksi virallinen kansallinen sähköinen tunnistautumisväline EU:n komissiolle [30]. Asetuksen mukaan lompakkosovellus on mobiilisovellus, joka mahdollistaa tunnistautumisen maiden rajat ylittävästi ja antaa käyttäjälle mahdollisuuden hallinnoida tunnistetietojaan sekä niiden käyttöä [30]. Lisäksi sovelluksessa on sähköinen allekirjoitusominaisuus [30]. Jäsenvaltioilla olisi velvollisuus tarjota vähintään yksi lompakkosovellus osana notifioitua sähköistä tunnistautumisjärjestelmää, jonka käyttö on vapaaehtoista ja maksutonta [30]. Asetuksen mukaan lompakkosovelluksia voi siis olla useita joko julkisten tai yksityisten toimijoiden toimesta kussakin jäsenvaltiossa tai kansainvälisesti [30]. Lompakkosovelluksen teknisempiin vaatimuksiin kuuluu, että lompakkosovellusten tulisi tarjota yhteinen rajapinta niiden käyttöä varten, tulee täyttää eIDAS High-varmuustason vaatimukset ja varmistaa, että tunnistetietojen tarjoajat voivat vahvistaa tietojen oikeellisuuden tietämättä tiedon käyttöpaikasta tai -tarkoituksesta [30]. Lompakkosovelluksen tulee siis toimia standardoidulla menetelmällä, jonka yksityiskohdista ei olla vielä sovittu, mutta jota rakennetaan paraikaa EU:n Toolbox-ryhmässä [30]. Lompakkoon luottaville osapuolille, kuten julkisen sektorin toimijoille ja yksityisen sektorin asiointipalveluille, tarjotaan mekanismi käyttäjien todentamiseen, eli keino pyytää käyttäjää todistamaan henkilöllisyytensä sovelluksen esittämää vastaavaksi [30]. Käytännössä tämä voi tapahtua esim. salasanan, PIN-koodin, kasvontunnistusteknologian tai sormenjälkitunnistimen perusteella [17]. Luottava taho on taho, joka aikoo sallia lompakkosovelluksen käytön sähköisiin palveluihinsa kirjautumisessa [30]. Tietyille tahoille, kuten julkisen sektorin palveluille, voidaan määrätä velvoite lompakkosovelluksen käyttöön, jolloin lompakkosovelluksen käyttö palvelun asioinnissa ei ole vapaaehtoista vaan pakollista [30]. Lompakkosovelluksen eetokseen kuuluu, että henkilön tunnistetiedot ovat yksilöiviä, aitoja ja luotettavia ja että sovellus on tietoturvallinen ja esteetön [30]. Vaatimustenmukaisuus osoitetaan sertifioinneilla [30]. Asetus jättää lompakkosovelluksen toiminnalliset yksityiskohdat ja tekniset standardit avoimiksi

[30]. Luottamustietojen tuominen identiteettilompakkoon tietoturvallisesti mahdollistetaan sähköisten attribuuttitodistusten avulla, jotka lisätään eIDAS-asetuksen soveltamisalaan sähköisen arkistoinnin, sähköisten allekirjoitusten sekä -tilikirjojen lisäksi [30]. Kaikki nämä muutokset sisältyvät uuteen eIDAS-asetukseen, jonka EU:n komissio aikoo hyväksyä vuoden 2022 loppuun mennessä [30].

Suomen kanta uudistettuun eIDAS-asetukseen ja sen sisältöön on ollut myönteinen [30]. Nähdään tärkeänä, että muutokset voidaan yhteensovittaa muun EU-lainsäädännön kanssa, kuten henkilötietojen suojaa koskevan säännöstön kanssa [30]. Sähköinen tunnistautuminen ja sähköiset asiakirjat ovat myös keskeisiä muiden EU-säädösten toimivuuden kannalta [30]. Yhdenvertaisuussyistä on tärkeää, että lompakkosovelluksen saavutettavuus taataan henkilöille, joilla ei ole älypuhelinta esim. tietokonesovelluksen tai verkkoselaimessa avattavan sovelluksen välityksellä [30]. Tässä työssä oletetaan, että loppukäyttäjällä on älypuhelin, joten tämän aiheen yksityiskohtia ei käsitellä tässä työssä. Myös yhteistyö julkisen ja yksityisen sektorin toimijoiden välillä nähdään tärkeänä Suomessa [30]. Lompakkosovellusta tulisi voida käyttää sekä sähköisessä että fyysisessä asioinnissa (esim. yrityksen verkkokaupassa ja liikkeessä) [30]. Hyväksytyillä sähköisillä attribuuttitodistuksilla, kuten lompakkosovelluksen henkilötiedoilla, olisi fyysisiä todistuksia vastaava oikeudellinen merkitys [30]. Lompakkosovelluksen toteutus-, käyttöönotto- ja ylläpitokustannukset tulevat olemaan merkittäviä, varsinkin jos jäsenmaat tuottavat lompakkosovelluksensa itse [30].

Viimeisenä huomiona EU:n komissio korostaa kokonaiskuvan näkemistä, sillä tämä on todennäköisesti viimeinen hetki säilyttää Euroopan Unionin kyky hallita digitaalista identiteettiä maailmanlaajuisella tasolla. Jos EU ei toimi nyt, kenttä jää avoimeksi digitaalisille alustajäteille kuten Google ja Facebook, jolloin EU:n komission kyky digitaalisen identiteetin ja sen käytön hallintaan heikkenee ja katoaa [30]. Näiden keskusteluiden lomassa on käyty myös keskusteluja identiteettilompak-

koon liitettävästä maksuominaisuudesta ja digitaalisesta eurosta, mutta käytännön toteutus tällaiselle ominaisuudelle on vielä epävarmaa [30]. Olemassaolevan infrastruktuurin määrä tällaiselle maksuominaisuudelle on rajallinen, itse identiteettilompakon kehitys ja implementaatio on etusijalla [30].

## 4.4 Identiteettilompakon allekirjoitusominaisuus

Sähköinen allekirjoittaminen on jo monien miljoonien eurojen arvoinen kasvava liiketoiminta [49]. Digitaalisen dokumentaation kasvava suosio, erityisesti COVID-19-epidemian aiheuttaman etätyökulttuurin jälkeen [49], on asettanut alan tuottoisaan kasvusuuntaan [49]. Kyseisen markkina-alan kasvu tuottaa mahdollisuuden integroida sähköinen allekirjoitusominaisuus eurooppalaiseen identiteettilompakkoon [30]. Tällaista signatuuria voidaan periaatteessa käyttää mihin tahansa digitaaliseen dataan, tiedostoon tai mediaan, kuten pdf- ja word-tekstitiedostoihin, äänitiedostoihin, sähköpostiviesteihin ja ohjelmistojen .exe-tiedostoihin. Digitaalinen allekirjoitus osoittaa allekirjoittajan identiteetin [50]. Sähköisten tiedostojen allekirjoittamisessa sillä pyritään osoittamaan kuka omistaa tai on luonut kyseisen tiedoston, mutta sähköisten dokumenttien, kuten sopimusten, allekirjoituksessa tärkeintä on varmistua allekirjoittajan identiteetistä [50]. Allekirjoitus toimii tositteena datan tai sovinnon alkuperästä [50]. Digitaalinen allekirjoitus perustuu luotetun tahon kohteelle myöntämään jaettuun identiteettiin, joka sidotaan dokumenttiin kryptografisia menetelmiä käyttämällä [50]. Kun tiedosto lähetetään, vastaanottaja voi helposti tarkistaa digitaalisen allekirjoituksen ja varmistua tiedoston alkuperästä [50]. Tästä syystä menetelmää hyödynnetään liiketoiminnassa arkipäiväisesti [49].

Sähköisen allekirjoituksen ydinideasta voidaan helposti muodostaa kytkös eurooppalaiseen identiteettilompakkoon [30]. Toistona, sähköinen allekirjoitus on kryptografisesti sidottu jaetun identiteetin tunnistetieto sähköisessä dokumentissa [50]. Kun eurooppalaiseen identiteettilompakkoon lisätään tiedostojen allekirjoittamiso-

minaisuus, tähän tarkoitukseen voidaan käyttää esimerkiksi identiteettilompakon sisältämää digitaalista henkilöllisyystodistusta. Esimerkiksi puhelimen omistaja voi ottaa kuvan kamerallaan, käyttää lompakkosovelluksen allekirjoitustoimintoa luodakseen digitaalisen allekirjoituksen ja jakaa sitten kuvan internetissä. Kuvatiedoston metadataan sisällytetty identiteettilompakon sähköinen allekirjoitus toimii todisteena kuvan ottajan henkilöllisyydestä muiden sähköisten allekirjoitusten tavoin. Lompakkosovelluksella sidottuja sähköisiä allekirjoituksia voidaan siis käyttää sertifikaatteina tiedon oikeellisuudesta ja todisteena allekirjoittajan identiteetistä [30].

Identiteettilompakon sähköisten allekirjoitusten toiminnan yksityiskohdat riippuvat lompakkosovelluksen teknisestä toteutuksesta. Gurulogic Microsystems Oy:n teknologiaa, jota käsitellään laajemmin kappaleessa 5, käytettäessä sähköiset allekirjoitukset tapahtuvat HTTP REST API-rajapinnan kautta. Dokumentti voidaan lähettää rajapintaan kryptografisesti julkisen avaimen salauksen kirjoittamista varten ja ladata allekirjoitettuna takaisin käyttäjän päätelaitteeseen metadatan kanssa tai ilman [51]. Allekirjoitettava dokumentti on alistettu ryhmäturvallisuudelle. Ryhmäturvallisuus mahdollistaa allekirjoitettavan dokumentin suojatun käsittelyn ja välittämisen helposti ja turvallisesti kaikille osapuolille. Dokumentin omistajakäyttäjä tai jäsen voi selvittää, onko tiedoston kopiota muokattu lataamisen jälkeen, eli luottamuksellisuus voidaan varmistaa [51]. Rajapinta antaa myös mahdollisuuden allekirjoitetun dokumentin poistamiseen ja muodostaa reaaliaikaisen lokin tiedoston elinkaaresta, johon tallennetaan mm. allekirjoituspyyntö ja poistopyyntö aikaleimoineen [51]. Kaikki pyynnöt tapahtuvat HTTPS-kutsujen välityksellä, jotka autentikoidaan PKA (public key authentication), OAuth2-tunnistautumismenetelmällä, jotka voidaan konfiguroida identiteettilompakkosovelluksen asetusten kautta [51]. [52]

## 4.5 Eurooppalaisen identiteettilompakon yhteenveto

Eurooppalainen identiteettilompakko on tulevaisuuden vahva sähköinen tunnistautumisjärjestelmä, jonka digitaalisen henkilöllisyystodistuksen avulla kohteen henkilöllisyys voidaan osoittaa sähköisesti fyysistä henkilöllisyystodistusta vastaavalla tasolla [31][30]. Identiteettilompakko perustuu eIDAS-asetukseen ja sen muutosehdotuksiin. Identiteettilompakko asettuu oletuksena turvallisuustasolle eIDAS High [30]. Jokaiselle EU:n kansalaiselle tulee tarjota edes yksi lompakkosovellus omassa jäsenmaassaan [30]. Asiointipalvelut ilmoittavat, kun he sallivat lompakkosovelluksen käytön palveluissaan, jolloin he muuttuvat luottaviksi osapuoliksi [30]. EU:n komissio voi velvoittaa asiointipalvelun hyväksymään lompakkosovelluksen käyttö sähköisissä palveluissaan [30]. Identiteettilompakko voidaan aktivoida esim. poliisilaitoksella paperista henkilöllisyystodistusta vastaan [31]. Henkilöllisyystodistuksen lisäksi lompakkoon voidaan lisätä muita henkilökohtaisia attribuutteja kuten ajokortti ja kirjastokortti, joilla oikeuksia ja tunnisteita voi osoittaa [30]. Lompakossa olevia tietoja voidaan esittää yksitellen, jotta ainoastaan vuorovaikutuksessa tarvittava tieto tuodaan esille [30]. Lompakkoa tullaan käyttämään mobiilisovelluksena, tietokonesovelluksena ja verkkopohjaisena palveluna [30]. Lompakon toiminnallisista yksityiskohdista vastaa lompakkosovelluksen tuottama valtio tai yritys [31]. Lompakkosovellus voisi korjata FTN:ssä ilmentyneet atomisaatio-, maksullisuus- ja luottamussuhdeongelmat tuomalla digitaaliset identiteetit lähemmäs EU:n hallinnan alaisuutta. Lompakolla tunnistautuminen ei veloita tunnistautumiskohtaista tunnistautumismaksua asiointipalvelulta ja luottamussuhde lompakon käyttäjän ja Digi- ja väestötietoviraston välillä ei sisällä yksityisten toimijoiden muodostamaa väliker-rosta [31][39].

# 5 Lompakon referenssiratkaisu: Starwindow® Identiteettilompakko

Kuten kappaleessa 4.3 todettiin, eurooppalaisen identiteettilompakkokonseptin alle voidaan sisällyttää useita lompakkosovelluksia, joista jokaisen jäsenmaan tulee käyttöönottaa vähintään yksi [30]. Kunkin lompakkosovelluksen teknisestä ratkaisusta ja toiminnallisuuden yksityiskohdista vastaa lompakkosovelluksen tuottava taho [31]. Tästä syystä teknisen toiminnallisuuden yksityiskohdat vaihtelevat lompakkosovelluksien välillä. Työnantajani, turkulaisen ohjelmistoyrityksen Gurulogic Microsystems Oy:n kehittämä Starwindow® Identiteettilompakko mahdollistaa yhden näistä digitaalisista identiteettilompakoista, jollaisia tullaan jatkossa näkemään valtioilta sekä yksityisiltä toimijoilta [53]. Jokaisen lompakkosovelluksen tekninen toteutus on ainutlaatuinen, joten tässä työssä esiteltävän Starwindow®-ratkaisun yksityiskohdat eivät välttämättä esiinny muissa ratkaisuissa.

## 5.1 Starwindow® Identiteettilompakon käyttöönotto

Starwindow® Identiteettilompakko soveltuu useisiin eri käyttötarkoituksiin, kuten sähköiseen tunnistautumiseen, digitaaliseen sisäänkirjautumiseen, digitaalisiin allekirjoituksiin, dynaamisiin varmenteisiin, sähköiseen valtuuttamiseen, digitaalisen

viestinnän ja tiedon salaamiseen sekä tietoturvallisen datansäilönnän applikaatioihin [53]. Starwindow® Identiteettilompakko tarjoaa loppukäyttäjälleen turvallisen, automatisoidun ja suojatun autentikaatiomenetelmän helpolla käyttöönotolla ja turvallisella käytöllä [54]. Tässä kappaleessa esitetään Starwindow® Identiteettilompakon käyttöönotto ja perustoiminnallisuudet alkaen yhden käyttäjän ja palveluntarjoajan välisestä kerroksesta ja päättyen järjestelmän skaalaukseen useampien käyttäjien ja palveluntarjoajien välillä.

### 5.1.1 Käyttäjän rekisteröinti ja attribuuttitodistus

Käyttäjän rekisteröinti on minkä tahansa identiteettilompakkosovelluksen peruskivi, johon koko järjestelmä perustuu, koska muutoin lompakolla ei voi olla käyttäjiä [30]. Samoin on Starwindow® Identiteettilompakossa, jossa käyttäjän lompakkosovelluksen käyttönotto voidaan jakaa kolmeen vaiheeseen: käyttäjän provisiointi, esirekisteröinti ja rekisteröinti [54]. On tärkeää ymmärtää, että pohjimmiltaan nämä kolme vaihetta ovat palveluntarjoajakohtaisia, koska ne tapahtuvat käyttäjän ja *yhden* Holvipalvelun välillä, joka on Holvipalveluntarjoajan ylläpitämä palvelu [54]. Käyttäjän provisioinnissa käyttäjälle muodostetaan User ID ja käyttäjävarmenne, jotka yhdessä muun käyttäjästä kerätyn olennaisen tiedon ja metadatan kanssa taltioidaan Holvipalveluun [54]. Viranomaisen tai muun valtuutetun tahon suorittama henkilöllisyyden todentaminen paikallisesti tai digitaalisesti voi olla vaatimus provisioinnin aloittamiselle käyttötapauksesta riippuen [54]. Provisiointia seuraa esirekisteröinti, jossa Holvipalveluun syötettävä adduser-komento muodostaa käyttäjän Holvin, jossa on käyttäjäarkisto, joka perustuu provisioinnissa taltioituihin tietoihin [54]. Tämä Holvi tallennetaan pilveen. Käyttäjän rekisteröinnissä käyttäjän henkilökohtaisessa päätelaitteessa olevaan Starwindow® asiakassovellukseen ladataan Holvi käyttäjäarkistoineen pilvestä, jolloin syntyy paikallinen Holvi [54]. Holvi allekirjoittaa sen sisältöineen latauksen yhteydessä, jotta asiakassovelluksen sisältämään käyttäjäarkis-

toon voidaan luottaa [54]. Näiden kolmen vaiheen jälkeen käyttäjän käyttäjäarkisto on provisioinnissa taltioituja tietoja lukuunottamatta tyhjä. Tyhjä käyttäjäarkisto mahdollistaa esim. kappaleessa 4.4 esitetyn tiedoston allekirjoittamisominaisuuden käytön käyttäjän User ID:n perusteella, mutta ei henkilötietojen osoittamista sähköisessä asioinnissa. Kertauksena, käyttäjän Holvi tallennetaan Holvipalveluun, joka on Holvipalveluntarjoajan ylläpitämä Holveja hallitseva palvelu [55]. Holvipalvelun voi tarjota palveluntarjoaja itse tai jokin kolmas osapuoli. Holvipalvelu pystyy mm. jäädyttämään ja poistamaan käyttäjien Holveja tapauksissa, joissa loppukäyttäjän päätelaite katoaa tai varastetaan, sekä lisäämään tai poistamaan käyttäjiä heidän välisissä ryhmissä [55]. Toisin sanoen Holvipalvelu on olemassa jo ennen käyttäjän ensimmäistä yhteyspyyntöä, mutta käyttäjän Holvi vasta Holvipalveluun esirekisteröitymisen jälkeen.

Käyttäjäarkiston tyhjyys ratkaistaan rekisteröinnin jälkeisellä attribuuttitodistuksen muodostamisella [56]. Attribuuttitodistuksen muodostamisessa hyväksytyn ja ei-hyväksytyn identiteettilompakkosovelluksen ero on merkittävä. Hyväksytty identiteettilompakkosovellus on EU:n jäsenvaltion virallisesti hyväksymä ja käyttöönottama hyväksytyn tahon tuottama lompakkosovellus, joka pystyy käsittelemään, taltioimaan ja osoittamaan hyväksytyn tason tietoja, kuten käyttäjän ikään liittyviä tietoja [57]. Hyväksytyn ja ei-hyväksytyn lompakkosovelluksen välillä ei tarvitse olla teknisiä eroavaisuuksia. Tämän työn kontekstissa Starwindow® Identiteettilompakkoa pidetään ei-hyväksyttynä lompakkosovelluksena. Ei-hyväksytyt henkilötiedot (PID) voidaan saada esim. nykyaikaisen vahvan sähköisen tunnistautumisen lopputuloksena [35] tai NFC:llä varustetusta passista [58], jos niille on rekisteröity oikeus myöntää PID-tietoa Eurooppalaiseen identiteettilompakkoon [57]. Ensimmäisessä tapauksessa käyttäjä tunnistautuu verkkopankkiin (esim. Nordea, Osuuspankki) verkkopankkitunnuksillaan, joita vastaan pankki palauttaa käyttäjän PID:n palveluntarjoajalle, joka on tässä tapauksessa käyttäjän henkilökohtainen Starwindow®

Identiteettilompakko [59]. Pankki siis palauttaa käyttäjälle luonnollisen henkilön [60] PID:in [35]. Toisessa tapauksessa käyttäjä lukee passissa olevan NFC-sirun päätelaitteellaan, jolloin passi palauttaa MRTD/MRZ-tiedot [61], joista päätelaite muodostaa käyttäjän luonnollisen henkilön PID:in [58]. PID välitetään käyttäjän pilvessä olevaan Holviin, jolloin tunnistuspalvelun (esim. verkkopankin) allekirjoittamista PID-tiedoista muodostetaan attribuuttitodistus, joka taltioidaan käyttäjän Holviin, pilvessä olevaan käyttäjäarkistoon, attribuuttiryhmänä, jonka Holvi allekirjoittaa [59]. Attribuuttitodistuksen avulla käyttäjä pystyy osoittamaan PID:iin tallennettuja tietoja erilaisissa asiointipalveluissa ja käyttötapauksissa [56]. Attribuuttiryhmään liitetään jäseneksi käyttäjä, jonka tiedoista on kyse, joka on ryhmän ainoa oletusjäsen [59]. Halutessaan käyttäjä voi muodostaa uuden attribuuttiryhmän jakaakseen attribuuttitodistuksen luku- ja käyttöoikeutta valituille entiteeteille, jotka tällöin pystyvät käyttämään kyseistä attribuuttitodistusta tunnistamis-, valtuuttamis- ja allekirjoitusvälineenä. Käyttäjän Starwindow® asiakassovellus noutaa attribuuttiryhmän pilvestä paikalliseen käyttäjäarkistoonsa [59]. Allekirjoitetun attribuuttitodistuksen sisältöön voidaan luottaa, koska PID ja sen sisältämät tiedot on vastaanotettu luotettavasta lähteestä. Hyväksytyn tason PID:in noutoa ei käsitellä tässä työssä, oletusarvoisesti EU:n jäsenmaa järjestää virallisen noutomenetelmän [57]. Käyttäjän provisioinnin, esirekisteröinnin, rekisteröinnin ja attribuuttitodistuksen muodostamisen jälkeen käyttäjällä on edellytykset omien henkilötietojensa osoittamiseen erilaisissa asiointipalveluissa. Huomaa, että yksittäisellä käyttäjällä voi olla useampia attribuuttitodistuksia, jotka hän on muodostanut tai joihin toinen käyttäjä on myöntänyt lukuoikeuden [62]. Yksi peruste attribuuttitodistuksen jakamiselle on esimerkiksi valtuutus, jossa henkilö on valtuuttanut toisen henkilön toimimaan omissa nimissään.

### 5.1.2 Käyttäjän ja palveluntarjoajan välinen asiointi

Yhden käyttäjän ja yhden palveluntarjoajan välinen tunnistautuminen ja asiointi on mahdollista vasta seuraavien vaatimusten täytyttyä:

1. Käyttäjän täytyy olla rekisteröitynyt kyseisen palveluntarjojan Holvipalvelun käyttäjäksi, eli hänellä täytyy olla oma Holvi palveluntarjoajan piirissä [56].

2. Käyttäjän on täytynyt suorittaa PID:n nouto esim. verkkopankkitunnistautumisen tai NFC:llä varustetun passin kautta. Muutoin hänellä ei ole henkilötietoja, joita osoittaa [59] [58].

3. Palveluntarjoajan on täytynyt rekisteröityä käytettävän Holvipalvelun luottavaksi osapuoleksi (ks. 4.3) [30]. Jos palveluntarjoaja hallitsee kyseistä Holvipalvelua, konditio täyttyy automaattisesti.

Näiden edellytysten täytyttyessä käyttäjä pystyy osoittamaan attribuutteja palveluntarjoajalle ja palveluntarjoaja pystyy vastaanottamaan sekä pyytämään niitä käyttäjältä. Molemmat osapuolet pystyvät luottamaan jaettuun tietoon, koska käyttäjän Holvi on allekirjoittanut ne tietoteknisen luottamuksellisuuden muodostamiseksi [59]. Käyttäjän ja palveluntarjoajan välinen asiointi voidaan jakaa seuraaviin kategorioihin:

1. Käyttäjä osoittaa attribuuttejaan paikallisesti offline-tilassa

   Käyttäjä kävelee henkilötietojen osoittamista vaativalle palvelutiskille, esim. optikon näöntarkastukseen, jossa käyttäjältä pyydetään sosiaaliturvatunnus. Oletetaan, että sosiaaliturvatunnus voidaan osoittaa ei-hyväksytyllä lompakkosovelluksella. Käyttäjä avaa asiakassovelluksessaan QR-koodin, jonka palveluntarjoaja lukee QR-koodilukijalla. Tällöin palveluntarjoaja saa käyttäjävarmenteen tietoonsa. Palveluntarjoaja pyytää käyttäjän sosiaalitunnusta hänen asiakassovellukseen tallennetusta allekirjoitetusta attribuuttitodistuksesta. Tiedot on tallennettu attribuuttitodistukseen avain:arvo-menetelmällä, eli

palveluntarjoaja pyytää tiettyä attribuuttiavainta vastaavaa arvoa käyttäjältä [63]. Käyttäjä hyväksyy tunnistamispyynnön asiakassovelluksessaan omalla henkilökohtaisella kredentiaalilla (esim. PIN-tunnuksella). Palveluntarjoaja vastaanottaa attribuutin, ja luottaa siihen, koska se on sähköisesti allekirjoitettu luotetun tahon toimesta.

2. Käyttäjä osoittaa attribuuttejaan paikallisesti online-tilassa

   Online-tilassa tapahtuva asiointi ei eroa merkittävästi offline-tilassa tehtävästä asioinnista. Tietojen varmentaminen pilvessä olevasta käyttäjän Holvin käyttäjäarkistosta on mahdollista ainoastaan online-tilassa. Lisäksi Holvin Blacklist-ominaisuuden täysi toiminnallisuus edellyttää online-tilaa. Blacklist toimii siten, että Holvin omistajan, palveluntarjoajan tai muun varteenotettavan tahon (esim. Poliisin) pyynnöstä käyttäjävarmenne, eli julkinen avain, voidaan merkitä hylättäväksi kaikessa asioinnissa. Holvi lähettää broadcast-viestin jokaiselle Holvipalveluun rekisteröityneelle käyttäjälle ja palveluntarjoajalle, jotka merkitsevät kyseisen käyttäjän automaattisesti mustaan listaan [64]. Jos käyttäjä siirtyy online-tilaan tämän jälkeen, hänen asiakassovelluksensa kyky käyttää käyttäjävarmennetta revokoituu välittömästi ja pysyvästi. Offline-tilassa oleva blacklistattu käyttäjä voidaan revokoida online-tilassa olevan palveluntarjoajan välityksellä niiden välisen asioinnin yhteydessä (esim. Bluetooth).

3. Käyttäjä tunnistautuu verkossa olevaan asiointipalveluun

   Käyttäjä avaa palveluntarjoajan verkkosivun, painaa kirjaudu sisään, ja valitsee Starwindow® Identiteettilompakon ruudulle aukeavista tunnistautumismenetelmistä. Asiointipalvelu noutaa käyttäjävarmenteen käyttäjältä saatua User ID:tä vastaan tai saa käyttäjävarmenteen suoraan käyttäjältä ja lähettää tunnistamispyynnön käyttäjävarmennetta vastaavaan asiakassovellukseen. Käyttäjä hyväksyy pyynnön henkilökohtaisella kredentiaalilla, jolloin asiakas-

sovellus lähettää Seal & Sign-viestin [65] palveluntarjoajan asiointipalveluun, jossa olevan julkisen avaimen ja Holvin allekirjoituksen perusteella palveluntarjoaja tietää, että viesti on validi, se koskee oikeaa henkilöä ja kirjautumisyritykseen voidaan luottaa. Käyttäjä kirjataan sisään.

Offline-tilassa asioidessa on syytä huomata, että jotkin identiteetintarjoajan toimesta tuoreutettavaksi määrätyt tiedot voivat deprekoitua pitkäaikaisen offline-käytön aikana. Tällöin attribuuttitodistukseen on sisällytetty ajanhetket, joiden välissä tieto on validi. Tällainen attribuuttitodistus voi päivittyä automaattisesti, kun käyttäjä on online-tilassa. Tarkat ehdot määrittelee identiteetintarjoaja.

### 5.1.3 Starwindow® LinkVault-tekniikka

Edellisissä kappaleissa esitettyjen toimien seurauksena käyttäjän on mahdollista tunnistautua ja osoittaa attribuuttejaan ainoastaan yhden palveluntarjoajan Holvipalvelun piirissä. Hyödyntääkseen tekniikkaa jonkin muun palveluntarjojan piirissä, esim. muun palveluntarjoajan asiointipalvelussa, käyttäjän pitäisi aloittaa koko prosessi alusta provisioitumalla tämän palveluntarjoajan käyttämään Holvipalveluun ja sitten rekisteröityä ja noutaa PID-tieto uuteen Holviin. Tämä rakenne aiheuttaisi suuria käytettävyysongelmia, jos Starwindow®-teknologian tarjoama LinkVault-tekniikka ei ratkaisisi sitä. LinkVault-tekniikalla Holvipalvelu pystyy linkittymään toiseen Holvipalveluun [66], jolloin mahdollistetaan web3-yhteiskäyttöpalvelut molempien Holvipalveluiden käyttäjien kesken. Käyttäjien välille muodostuu tietotekninen luottamusverkosto, jonka ansiosta kahden eri Holvipalvelun käyttäjät pystyvät tarjoamaan toisilleen palveluita ja toimintoja. Yhden Holvipalvelun käyttäjä pystyy esimerkiksi muodostamaan ryhmän, jonka jäseninä on ulkopuolisten linkitettyjen Holvipalveluiden käyttäjiä, tai lisäämään ulkoisten Holvipalveluiden käyttäjiä jäseniksi omaan attribuuttiryhmäänsä. Tärkein LinkVault-tekniikan mahdollistama ominaisuus on se, että yhden Holvipalvelun käyttäjä pystyy tunnistautumaan ja

asioimaan toista Holvipalvelua käyttävän palveluntarjoajan asiointipalveluissa niiden välisen linkin kautta. Palveluntarjoaja pystyy myös pyytämään attribuutteja ulkoisen Holvipalvelun käyttäjiltä edellisessä kappaleessa esitetyn mallin mukaisesti. Tapauksessa, jossa käyttäjä on lisätty ulkoisessa Holvipalvelussa olevaan ryhmään, ryhmä noudetaan aina omasta Holvipalvelusta, joka noutaa ryhmän linkitetystä ulkoisesta ryhmän omistajan Holvipalvelusta, eli sieltä, minne ryhmä on alkujaan luotu. Noudoissa käytetään Trusted-tason Holvipalveluiden välisiä tunnuksia, jotka asetetaan linkityksen yhteydessä, jolloin käyttäjien tunnuksia ei tarvita oman Holvipalvelun ulkopuolella. Käyttäjän tunnuksia ei tarvita, koska linkitetty Holvipalvelu palauttaa ryhmän suojattuna vastaanottajakäyttäjän käyttäjävarmennetta vastaan, jonka käyttäjä voi avata oman Holvipalvelunsa sisällä. [67]

Holvipalveluiden linkit muodostavat ketjuja ja verkostoja, joissa jokainen ketjun jäsen pystyy keskustelemaan kaikkien muiden ketjun jäsenien kanssa. Jokaisen Holvipalvelun ei siis tarvitse erikseen linkittyä jokaisen muun Holvipalvelun kanssa. Eurooppalaisen identiteettilompakon tavoitteiden mukaisesti Euroopan kansalaisen kansallinen, jopa kansainvälinen vahva sähköinen tunnistautuminen voidaan mahdollistaa hänen kotiholvipalvelustaan LinkVault-tekniikkaa käyttämällä. Käyttäjä pystyy hallitsemaan omia tietojaan omassa Holvipalvelussaan ja hyödyntämään niitä kansainvälisissä palveluissa LinkVault-tekniikan mahdollistamien verkostojen välityksellä. [67]

## 5.2 Starwindow®-teknologian edut

Starwindow®-teknologiassa käyttäjän ja palvelun välille muodostuu täysin automaattisella avaintenhallinnalla varustettu suora luottamussuhde, joka minimoi loppukäyttäjältä vaadittujen operaatioiden määrää. Näin vähennetään inhimillisten virheiden aiheuttamien turvallisuusriskien mahdollisuutta. Suoran luottamussuhteen turvallisuus perustuu julkisen salauksen kryptografiaan, englanniksi PKI (Public

Key Infrastructure) [52], johon Starwindow®-teknologia tarjoaa PKI-järjestelmään nähden lisäturvaa avainmateriaalien korkean entropian ennustamattoman satunnaisuuden myötä [68]. Luottamussuhteita voidaan muodostaa käyttäjän ja Holvipalveluiden sekä palveluntarjoajien välille. Käyttäjän ja Holvipalvelun välisen luottamussuhteen muodostaminen vaatii kertaluontoisen käyttöönottoprosessin, jossa käyttäjä rekisteröityy Holvipalveluun henkilökohtaisella kredentiaalilla, kuten PIN-tunnuksella. Tämä voidaan suorittaa esim. siinä yhteydessä, kun käyttäjä rekisteröityy Holvipalveluun kappaleen 5.1.1 mukaisesti. Käyttäjän täytyy olla rekisteröitynyt Holvipalveluun, jotta hän pystyy muodostamaan luottamussuhteen samaa Holvipalvelua hyödyntävän palveluntarjoajan kanssa. Kun käyttäjä kirjautuu palveluntarjoajan asiointipalveluun ensimmäistä kertaa, kummallakaan ei ole julkisia avaimia, joiden perusteella tunnistaa toisensa, eli luottamussuhdetta ei ole. Käyttäjän kertaluontoinen tunnistaminen tai kirjautuminen esim. asiakaspankin tunnistuspalveluun muodostaa luonnollisen henkilön attribuuttitodistuksen, joka käy palveluntarjoajalle. Käyttäjän ei tarvitse tunnistautua seuraavan kerran kun hän asioi palveluntarjoajan kanssa, koska tunnistuspalvelun aiemmin sähköisesti allekirjoittama attribuuttitodistus varmistaa käyttäjän henkilöllisyyden. Käyttäjän ja palveluntarjoajan välillä on tällöin suora luottamussuhde. Teknologian tavoitteena on, että käyttäjä pystyy hyödyntämään kyseisen palveluntarjoajan palveluja suoran luottamussuhteen turvin kirjautumatta uudelleen, paitsi avainten vanhennuttua. Suora luottamussuhde mahdollistaa käyttäjän, Holvipalvelun ja palveluntarjojan monenkeskisen automaattisen autentikaation heidän välisten julkisten avaimien perusteella. Tällä tavalla automatisoitu ratkaisu on käyttäjäystävällinen, helppokäyttöinen ja turvallinen. Suoran luottamussuhteen ansiosta järjestelmään linkitettyjen palveluiden käyttäminen on mahdollista jopa offline-tilassa ensimmäisen autentikaation jälkeen, koska palvelun luottamus käyttäjän henkilöllisyyteen perustuu verkkoyhteydestä riippumattomaan suoraan luottamussuhteeseen. Luottamussuhde perustuu

yhteen tunnistautumiskertaan, mikä tekee järjestelmästä kustannustehokkaan. [53]

Holvipalvelun ja Holvin kautta välitetty data on aina salattu. Jokainen datapaketti salataan omalla ainutkertaisella salausavaimellaan, jota ei paljasteta Holvin ulkopuolelle missään vuorovaikutuksen vaiheessa [53]. Salausavainten luomiseen Holvipalvelu tarvitsee avainmateriaalia. Avainmateriaalit ladataan kertaluontoisesti Gurulogic Microsystems Oy:n patentoitua menetelmää käyttäen, salattuna [69]. Avainmateriaalit ovat raaka-aineita, joiden perusteella Holvi pystyy johtamaan käytännössä rajattoman määrän ainutlaatuisia, tosisatunnaisuuteen perustuvia salausavaimia standardoituihin kryptografia-algoritmeihin perustuen [53]. Avainmateriaalit ladataan kertaluontoisesti Holvipalvelun alustuksen yhteydessä verkon välityksellä, joka tapahtuu vahvalla yhteyden ja sisällön salauksella [53]. Järjestelmä ei koskaan jaa avaimia tai niihin liittyvää materiaalia internetin välityksellä ilman vahvaa salausta [53]. Käytännössä ratkaisun turvallisuus perustuu avainten yksilölliseen tosisatunnaisuuteen, eikä siten ole murrettavissa laskennallisesti raa'alla voimalla (brute force), koska ennustamatonta tosisatunnaisuutta ei ole tuotettu matemaattisesti [68]. Järjestelmä ei koskaan lähetä salausavaimia salatun datan yhteydessä, mikä vähentää potentiaalisten tietoturvariskien määrää edelleen [70]. Symmetrisiä salausavaimia ei jaeta asiakassovelluksen ja Holvin tai Holvipalvelun välisessä viestinnässä [53]. Holvipalvelulla ei ole minkäänlaista luontaista pääsy- tai lukuoikeutta käyttäjien Holveissa olevaan salattuun dataan, eli suurimpaan osaan käyttäjien tiedoista. Käyttäjän tiedot ovat aina salattu yksilöllisesti perustuen aiemmin mainittuun automatisoituun Starwindow®-avaintenhallintaan. Tämän rakenteen ansiosta käyttäjä on oman datansa herra; tieto ei poistu holvista ilman käyttäjän suostumusta.

Holvi tallentaa käyttäjän datan patentoituun suojattuun käyttömuistiin, johon kohdistuvat tallennus- ja lukuoperaatiot suoritetaan aina yhden säikeen alla ilman keskeytyksiä [71]. Tämä suojatun käyttömuistin teknologia suojaa järjestelmän käsittelemän sensitiivisen tiedon, jota laite lukee tai kirjoittaa suoritusaikaisessa muis-

tissa (I/O) [53]. Data tallennetaan käyttäjäkohtaisella yksilöllisellä salausavaimella, jonka Holvi on generoinut tallennusprosessin alussa avainmateriaalin määrityksien mukaisesti [53]. Automatiikka sijoittaa salatun datan eri muistialueisiin turvallisuuden parantamiseksi, jotta salatun datan sekä salaukseen käytettyjen algoritmien yhtäaikainen hallinta kolmannen osapuolen toimesta olisi mahdollisimman hankalaa [71]. Eurooppalaisen identiteettilompakon käsitteiden mukaisesti Starwindow®-teknologian asiakassovellus vastaa lompakkosovellusta ja Holvipalvelu palveluntarjoajan taustapalvelua. Starwindow®-teknologia tarjoaa käyttötarpeesta riippumatta tehokkaan ratkaisun eurooppalaisen identiteettilompakon esittämiin haasteisiin.

## 5.3 Starwindow®-teknologian yhteenveto

Starwindow® Identiteettilompakko mahdollistaa käyttäjän rekisteröinnin ja ydinhenkilöllisyyden taltioinnin palveluntarjoajan Holvipalvelussa olevaan Holviin, joka mahdollistaa mm. PID-informaation osoittamisen ja tiedostojen allekirjoitusominaisuuden kyseisen palveluntarjoajan piirissä. Holviin tallennetaan käyttäjän hyväksytty tai ei-hyväksytty PID allekirjoitettuna attribuuttitodistuksena. Palveluntarjoja pystyy pyytämään käyttäjää osoittamaan attribuutteja ja käyttäjä pystyy osoittamaan attribuuttejaan palveluntarjoajille paikallisesti offline- ja online-tilassa tai verkon välityksellä. Holvipalvelut pystyvät linkittymään toisiinsa LinkVault-tekniikan ansiosta, jolla mahdollistetaan organisaatioiden väliset tunnistautumisverkostot. Osapuolien välinen kommunikaatio on aina salattu palveluntarjoajakohtaisilla avainmateriaaleilla. Yksikään Starwindow®-identiteettialustan komponentti ei pysty lukemaan Holvissa olevia tietoja ilman käyttäjän suostumusta. Järjestelmän automaattinen avaintenhallinta vähentää inhimillisten virheiden mahdollisuutta tunnistautumisprosessin aikana, ja asiakassovelluksen ja palveluntarjoajan välille muodostuva suora luottamussuhde ensimmäisen tunnistautumisen yhteydessä mahdollistaa tulevat autentikaatiot jopa offline-tilassa.

# 6 Identiteettilompakon käytännön huomioita

Tässä kappaleessa identiteettilompakon toimintaa käsitellään käytännönläheisestä näkökulmasta, jotta aiemmissa kappaleissa sivuutettuja aiheita voidaan nostaa esiin. Alaotsikoiden alla esitetään uudenlaisia keinoja hyödyntää identiteettilompakkoratkaisun mahdollistamaa vahvaa sähköistä tunnistautumista sekä esitetään niiden analysointiin perustuvia johtopäätöksiä. Lisäksi kappaleessa käsitellään erilaisia keinoja identiteettilompakkotunnistautumisen väärinkäytön ehkäisemiseksi. Kappaleen sisältö perustuu kirjoittajan omiin ajatuksiin ja johtopäätöksiin.

## 6.1 Sovelluksen tunnistautuneen tilan väärinkäyttö

Sovellus tai palvelu siirtyy tunnistautuneeseen tilaan, kun käyttäjän tunnistautuminen hyväksytään, ja pysyy tunnistautuneessa tilassa kunnes käyttäjä uloskirjautuu tai sessio päättyy esim. palveluntarjoajan aikakatkaisuun. Tunnistautuneessa tilassa olevaa sovellusta voidaan pitää alttiina väärinkäytölle. Näitä, sekä muita tunnistautuneen tilan implikaatioita voidaan tarkastella sosiaalisen median palveluiden näkökulmasta. On vaikea ymmärtää, miksi vahva sähköinen tunnistautuminen sosiaalisen median palveluihin ei aina ole mahdollista, sillä tällaisella ominaisuudella on käyttämätöntä potentiaalia. Tämä idea ei perustu siihen, että palvelun käyttäjätunnukset vaihdetaan käyttäjätunnus/salasanaparista identiteettilompakkosovelluksen mukai-

seksi tunnistautumiseksi, vaan se perustuu käyttäjälle vaihtoehtoiseen korkeamman tunnistautumistason tilaan, johon palvelu siirtyy, kun siihen kirjaudutaan eurooppalaisella identiteettilompakolla. Tämä ylikirjautunut tila voidaan kliseisesti nimetä "superkirjautumiseksi". Superkirjautuminen mahdollistaisi henkilöllisyyden todentamiseen perustuvan ylimääräisen luottamussuhteen muodostamisen käyttäjän ja muiden käyttäjien välille. Prosessi etenee seuraavasti:

1. Käyttäjä valitsee kirjautumisen lompakkosovelluksella käyttäjätunnusten sijaan.

2. Käyttäjä tunnistautuu palveluun.

3. Palvelu superkirjautuu, jolloin jokainen istunnon aikana lähetetty viesti leimataan erityisellä ikonilla.

Superkirjautuneessa tilassa lähetetty viesti sisältäisi erityisen leiman, joka näkyy kaikille palvelun käyttäjille. Leima ilmaisee, että lähetyshetkellä viestin lähettäjä oli tunnistautunut jollakin vahvalla sähköisellä tunnistautumismenetelmällä, kuten lompakkosovelluksella. Ominaisuuden turvallisuushyödyt kohdistuvat sekä viestin lukijoihin että lähettäjään. Leiman olemassaolo kasvattaisi lukijan uskoa viestin alkuperään, joka vahvistaa lukijan ja viestin lähettäjän välistä luottamussuhdetta. Lukija ymmärtää välittömästi, että pystyäkseen lähettämään viestin, lähettäjän tuli pystyä kirjautumaan palveluun henkilöllisyyden todentavalla tavalla, joka on vaikeampaa kuin kirjautuminen käyttäjätunnus/salasanaparilla [4] [44]. Ominaisuus tähtää siihen, että viestin lähettäjän fyysisen ja digitaalisen identiteetin linkki varmistetaan palvelun kirjautumishetkellä. Tästä syystä todennäköisyys siihen, että viesti on lähetetty tilin omistajan toimesta on suurempi kuin tavallisessa viestissä. Täten lukijalla on suurempi luottamus siihen, että viestin lähettäjä on se henkilö, joka hän väittää olevansa. Tuntemattoman henkilön kanssa keskustellessa käyttäjä voi pyytää häntä superkirjautumaan todistaakseen "ruudun toisella puolella"olevan

henkilön henkilöllisyyden. Ominaisuudessa on kaksi poikkeustilannetta, joissa henkilöllisyyden todentaminen epäonnistuu. Ensimmäinen on tilanne, jossa luvaton henkilö tunnistautuu palveluun toisen henkilön identiteettilompakolla ja toisessa tilanteessa uhrin läheisyydessä oleva henkilö nappaa superkirjautuneessa istunnossa olevan päätelaitteen ja kirjoittaa viestin sen avulla.

On syytä huomata, että käyttäjien ja viestien leimaaminen tunnistautumisprosessiin perustuvalla varmistuksella ei ole täysin uusi ajatus, ainoastaan rajallisesti implementoitu nykypäivän sosiaalisessa mediassa. Twitter on vuodesta 2009 alkaen hyödyntänyt tilien vahvistamisjärjestelmää, jonka ansiosta sivuston lukijat voivat erottaa todelliset tilinomistajat huijareista ja parodioista [72]. Vahvistusjärjestelmän varmistamaan tiliin liitetään sininen valintamerkki Twitterin toimesta, joka osoittaa lukijoille, että tili on Twitterin hyväksymä ja siten todellinen julkisuuden henkilöä, yritystä tai brändiä edustava käyttäjätili [72]. Valitettavasti sininen valintamerkki leimaa ainoastaan käyttäjän tilin, eli se on Twitter-tilin pysyvä passiivinen ominaisuus, joten kunhan luvaton käyttäjä kykenee kirjautumaan kyseiselle tilille, hänen lähettämiensä viestien uskottavuus on tilin omistajaa vastaava. Esimerkiksi heinäkuussa 2020 Twitter lukitsi kaikkien vahvistettujen tilien oikeuden lähettää viestejä hetkellisesti, koska rajalliseen määrään niistä oli hyökätty, muodostaen merkittävän turvallisuusriskin [73]. Sinisen valintamerkin saaminen ei myöskään ole mahdollista, jos hakijan henkilöllisyyden yhteiskunnallisen merkityksellisyys on vähäinen [72], eli valtaosa Twitterin käyttäjistä ei pysty hankkimaan sinistä valintamerkkiä itselleen [72]. Viimeinen haaste on, että sininen valintamerkki on Twitter-alustan ominaisuus, jota varten hakijan täytyy *kerran* lähettää oma henkilöllisyystodistuksensa [72] Twitterille, eli tunnistautumista ei tarvitse toistaa jokaisen kirjautumisen, istunnon tai päivityksen yhteydessä, toisin kuin aiemmin esitetty sosiaalisen median superkirjautumisominaisuus vaatisi. Huomaa, että Twitterin uusi omistaja on sekoittanut sinisen valintamerkin merkitystä Twitter Blue-ominaisuuden julkaisun seurauksena,

mutta ominaisuus on edelleen olemassa alkuperäisessä merkityksessään [74].

Superkirjautumisominaisuus ratkaisisi nämä haasteet vaatimalla tunnistautumisen eurooppalaisella identiteettilompakkosovelluksella jokaista istuntoa [75] kohden, jossa käyttäjä tahtoo ominaisuutta käyttää. Tällöin henkilöllisyyden varmistaminen ei ole käyttäjätilin pysyvä ja passiivinen ominaisuus, vaan istunnon aktiivinen ominaisuus [75], joka haihtuu istunnon päätyttyä. Kirjautuminen ilman vahvaa sähköistä tunnistautumista ei tuota superkirjautunutta tilaa riippumatta siitä, onko tilille superkirjauduttu aiemmin vai ei. Implementaatio on siis turvallinen tästä näkökulmasta, eikä se mahdollista samankaltaisia hyökkäyksiä kuin Twitter koki heinäkuussa 2020 [73]. Superkirjautuminen välttää myös kolmannen haasteen joka rajoittaa siniselle valintamerkille kelpaavien käyttäjätilien määrää sen prioriteetin perusteella [72]. Haaste syntyy siitä, että sininen valintamerkki on Twitterin hallitsema ominaisuus, joka täytyy hankkia hakemuksella [72], eli se on tilikohtainen ominaisuus. Twitter pystyy käsittelemään ainoastaan rajallisen määrän tilejä yhtäaikaisesti, siksi ominaisuutta priorisoidaan yhteiskunnallisesti merkittäviin käyttäjiin [72]. Superkirjautumisominaisuus ei olisi tilikohtainen ominaisuus, vaan koko alustan kattava ominaisuus. Koska sähköinen tunnistautuminen on eurooppalaisen identiteettilompakon mahdollistama ja ylläpitämä, ominaisuuden implementointi kaikille palvelun käyttäjille voi olla mahdollista, sillä se ei vaadi erillisiä tilikohtaisia resursseja palveluntarjoajalta, eli Twitteriltä.

Superkirjautumisominaisuus sisältää yhden ongelman, josta voisi muodostua epidempia ominaisuuden julkaisun yhteydessä. Kuten aiemmin esitettin, on kaksi tilannetta, joissa luvaton käyttäjä voi lähettää leimalla varustettuja viestejä toisen käyttäjän nimissä.

1. Käyttäjä pystyy valheellisesti tunnistautumaan uhrin digitaalisella identiteettillä.

2. Käyttäjä pystyy kirjoittamaan ja lähettämään viestin uhrin päätelaitteella

superkirjautuneen istunnon aikana.

Näistä ensimmäiseen voidaan vaikuttaa kasvattamalla tunnistautumiseen tarvittavan tiedon määrää ja/tai -laatua. Tämä ei ole asiointipalvelun päätettävissä, vaan se on eurooppalaisen identiteettilompakkoon ja lompakkosovellukseen sisällytetty ominaisuus [30]. Toinen tapaus on asiointipalvelun tai jopa yksittäisten käyttäjien päätettävissä. Tässä tapauksessa hyökkääjä ohittaa vahvan sähköisen tunnistautumisen tarpeen kokonaan ja pääsee käsiksi valmiiksi superkirjautuneeseen tiliin. Äkilliset puhelimen omistajuuden muutokset voidaan jakaa kolmeen ryhmään [76]:

1. Puhelin varastetaan koska omistaja jätti sen vartioimatta julkiseen ympäristöön.

2. Puhelin varastetaan asunnosta tai ajoneuvosta murtautumisen yhteydessä.

3. Puhelin varastetaan omistajan käsistä, taskusta, käsilaukusta tai kassista.

Näistä tyypillisin tapaus, joka voi kattaa jopa puolet kaikista puhelinvarkauksista [76], on ensimmäinen tapaus, jossa puhelin jätetään vartioimatta julkiseen paikkaan. Loput varkaustapaukset jakautuvat kahden muun kategorian kesken [76]. Tapaukset voidaan jaotella ja eliminoida niiden luonteen perusteella. Tapauksessa, jossa puhelin varastetaan murtautumisen yhteydessä, on päivänselvää, että puhelin on pysynyt paikallaan ja käyttämättömänä vähintään sen minuutin ajan jonka murtautuminen edellyttää [77]. Tapaukset, joissa puhelin varastetaan omistajan taskuista tai laukusta voidaan myös jaotella samaan ryhmään. Näissä tapauksissa puhelimen omistajan periaatteellisuus on kriittisessä roolissa. Jos puhelimen omistaja sulkee näytön aina, kun hän laskee sen käsistään tai asettaa automaattisen aikarajoituksen näytön sulkemiselle ja käyttää lukitusnäyttöä [78], puhelin voi olla väärinkäyttäjän näkökulmasta käyttökelvoton jo silloin, kun hän saa sen käsiinsä. Lisäksi asiointipalvelu itse voi asettaa automaattisen aikakatkaisun toimettomalle superkirjautumiselle, jolla taataan aikarajoitus tälle väärinkäytön mahdollisuudelle [77]. Jäljellä olevat tapaukset,

joissa puhelin jätetään vartioimatta julkiseen ympäristöön tai varastetaan omistajan käsistä, muodostavat kriittisen turvallisuusriskin, jossa aikaikkunaa automaattisille näytön tai istunnon sulkemisille ei ole taattu. Kun puhelin jätetään vartioimatta, omistaja voi sulkea näytön tai päättää superkirjautuneen istunnon ennen puhelimen hylkäämistä, mutta näin ei aina tapahdu [78]. Omistajalla ei myöskään välttämättä ole mahdollisuutta näytön sulkemiseen, kun puhelin riistetään hänen käsistään. Pöydälle jätettyä aukinaista puhelinta voi käyttää kuka tahansa, se ei pyydä lukituksen avaamista millään menetelmällä, eikä se tunnista käyttäjän muuttumista. Väärinkäyttäjä voi siis käyttää superkirjautunutta tilaa yhtenevästi laitteen todellisen omistajan kanssa.

Näiden vaaratilanteiden välttämisessä ensimmäinen päätös liittyy toimettoman superkirjautumistilan automaattiseen aikakatkaisuun, joka on passiivinen turvallisuutta parantava ominaisuus. Tällöin superkirjautunut tila päättyy, esim. tapauksessa, jossa aukinainen puhelin odottaa pöydällä liian pitkän ajan. Mitä lyhyemmäksi aikakatkaisu määritellään, sitä todennäköisemmin aikakatkaisu tapahtuu ennen väärinkäytön alkua [77]. Vastaavasti sitä useammin puhelimen omistajan täytyy uudelleentunnistautua normaalin käytön aikana jos laitteen käyttö on katkonaista. Ominaisuus täytyy tasapainottaa turvallisuuden ja mukavuuden välillä. Kaikkein turvallisin mahdollinen vaihtoehto on, että asiointipalvelu pyytää käyttäjää tunnistautumaan erikseen jokaista viestiä varten. Kaikkien mukavin vaihtoehto on, että käyttäjä tunnistautuu kerran eikä tunnistautunut tila pääty koskaan automaattisesti. Erillinen tunnistautuminen jokaista viestiä varten on niin epäkäytännöllinen ratkaisu, että palvelun käyttäjät todennäköisesti välttelisivät ominaisuuden käyttöä [79]. Vastaavasti pysyvästi tunnistautunut istunto ei saavuta ominaisuudelle asetettuja turvallisuustavoitteita, koska se ei hyödynnä joidenkin varkaustapausten myöntämää aikaikkunaa [77]. Näiden äärimmäisten ratkaisujen välimaastosta löytyy mm. seuraavat vaihtoehdot:

1. Tunnistautuminen päätetään, kun päätelaitteen näyttö sammuu (mobiili).
2. Tunnistautuminen päätetään käyttäjän toimettomuuden perusteella.
3. Tunnistautumisella on aikarajoitus käyttäjän aktiivisuudesta riippumatta.
4. Tunnistautuminen täytyy uusia aina, kun sovellus avataan (mobiili).

Vaihtoehto kolme tarkoittaa, että superkirjautumiselle asetetaan käyttäjän aktiivisuudesta riippumaton kiinteä aikarajoitus. Käyttäjän tulee tunnistautua uudelleen tasaisin väliajoin tilan ylläpitämiseksi. Ominaisuuden turvallisuushyöty on, että se asettaa kiinteän aikarajan myös väärinkäytölle, eli ryöstäjä voi aiheuttaa vahintoa vain rajallisen ajan. Tavanomaisessa käytössä ominaisuuden aiheuttama rasitus on toistuvaa ja voi johtaa ominaisuuden käytön vähentymiseen [79]. Vaihtoehto kaksi toimii samalla periaatteella, mutta tunnistautumisen aikarajoitus on dynaaminen. Tunnistautuminen ei pääty, kun sovellus on aktiivisessa käytössä, mutta haihtuu ennalta määritellyn ajan kuluttua, kun sovellusta ei käytetä. Sovelluksen käyttäminen kattaa päätelaitteen syötteet, esim. näppäimistöt, hiiret, kosketusnäytöt ja etäkäytön. Aktiivisuuteen sidottu aikarajoitus eliminoi kiinteän aikarajan aiheuttamaa toistuvaa rasitusta sillä kompromissilla, että myös väärinkäyttäjä pysyy tunnistautuneena ikuisesti, jos hän käyttää sovellusta aktiivisesti. Kummassakin tapauksessa automaattinen aikakatkaisu varmistaa, ettei tunnistautuminen ole pysyvä päätelaitteen toimettomassa tilassa. Vaihtoehdot yksi ja neljä päättävät tunnistautuneen tilan istunnon tilan perusteella. Istunnolla tarkoitetaan yhtenäistä aikaväliä sovelluksen avaamisen ja sulkemisen välillä [75]. Vaihtoehdossa yksi istunto päättyy, kun käyttäjä sulkee puhelimen näytön, johon palvelu reagoisi päättämällä tunnistautuneen tilan automaattisesti. Tällöin omistaja voi käyttää sovellusta, sulkea näytön, jättää puhelimen valvomatta julkiseen tilaan ja tietää, ettei ainakaan superkirjautunutta istuntoa voi varastaa. Vaihtoehtojen yksi ja neljä ero on pääosin tekninen. Käytännössä määritellään, onko superkirjautuneen tilan automaattinen päättämi-

nen tehokkaampaa sovelluksen avaamis- vai sulkemishetkellä. Loppukäyttäjän näkökulmasta kumpikin menetelmä tuottaa saman lopputuloksen: tunnistautunut tila päättyy, kun sovellus ei ole aukinainen puhelimen tai muun päätelaitteen näytöllä. Näiden menetelmien implementaatio tietokonesovelluksiin tai web-pohjaisiin käyttöliittymiin voi olla haasteellista. On mahdollista, että automaattisen uloskirjautumisen peruste voidaan antaa käyttäjän päätettäväksi sovelluksen asetuksissa. Tällöin käyttäjä voisi itse millä perusteella superkirjautunut istunto päätetään ja kuinka kauan puhelimen täytyy olla toimettomana uloskirjautumisen aiheuttamiseksi.

## 6.2 Tunnistautuminen päätelaitteeseen

Toinen sovellutusmahdollisuus lompakkotunnistautumiselle on päätelaitteeseen kirjautuminen. Joihinkin päätelaitteisiin tallennettu tieto on hyvin arvokasta ja tiedon päätyminen vääriin käsiin nähdään yksilön tai yrityksen näkökulmasta kriittisenä tietoturvariskinä [80]. Tällainen päätelaite voi esimerkiksi olla työpaikan pöytätietokone tai työpaikan tarjoama puhelin, johon on tallennettu yritykselle kriittistä tietoa [80]. Tällaisiin kriittistä tietoa sisältäviin laitteisiin ei aina kirjauduta matalan tason tunnistautumismenetelmällä kuten käyttäjätunnuksella ja salasanalla, vaan työpaikan edellyttämällä vahvemmalla tunnistautumisella, kuten äly- tai toimikortilla, jonka työntekijä syöttää tietokoneeseen kirjautumisen yhteydessä [81]. Toimikorttiin tallennettu siru toimii tunnisteena tietokoneen käyttäjän henkilöllisyydestä. Tämä ei kuitenkaan ole käytännönläheinen lähestymistapa, kun vahvaa sähköistä tunnistautumista halutaan markkinoida kuluttajille [82], eikä älykortinlukijan implementointi kaikkiin laitteisiin olisi välttämättä edes mahdollista kortinlukijan sekä siihen syötettävän kortin koon seurauksena. Äärimmäisenä esimerkkinä kortinlukijan integrointi älypuhelimeen voidaan nähdä järjenvastaisena. Näistä syistä voi olla järkevää harkita vahvoja ohjelmistopohjaisia tunnistautumismenetelmiä rakenteellisten menetelmien sijaan.

Tämän idean lopputuotteessa identiteettilompakolla tunnistautuminen olisi vain yksi tunnistautumismenetelmä muiden ohella, joiden väliltä loppukäyttäjä voi valita haluamansa, erityisesti mobiilimarkkinoilla. Parhaassa mahdollisessa integraatiossa ominaisuus on lisätty osaksi Android- tai iOS-puhelimen käyttöjärjestelmää. Tällöin puhelimen ruudun auetessa kirjautumiseen ei vaadita PIN-koodia, kaksiuloitteista muotoa tai sormenjälkeä, vaan ruutua painamalla laite lähettää sähköisen tunnistautumispyynnön toiseen laitteeseen, jossa identiteettilompakon päätesovellus sijaitsee. Jos käyttäjällä on esimerkiksi kaksi älypuhelinta, hän voi rekisteröidä toisen puhelimensa kirjautumisvälineeksi. Käyttäjä avaa toisen puhelimensa ja hyväksyy siihen saapuneen sähköisen tunnistautumispyynnön, jolloin lukittu puhelin aukeaa käyttövalmiiksi. Kirjautumismenetelmä on hyvin turvallinen, koska kirjautuminen turvattuun laitteeseen on mahdollista ainoastaan jos kirjautuja omistaa molemmat laitteet ja pystyy hyväksymään sähköisen tunnistautumispyynnön lompakkosovelluksessa. Tämä tunnistautumismenetelmä perustuu johonkin, joka kohteella täytyy olla (puhelin) ja johonkin, jonka kohteen täytyy tietää (identiteettilompakolla tunnistautuminen) [44]. Järjestelmän implementaatio ei ainakaan teoriassa vaadi rakenteellisia muutoksia tunnistautumismenetelmää hyödyntävään laitteeseen, sillä ratkaisu on täysin ohjelmistopohjainen. Valitettavasti puhdas ohjelmistoratkaisu tuottaa seuraavat kaksi ongelmaa:

1. Ratkaisu on hankala.

2. Biometrinen ratkaisu on turvallisempi.

Näistä molemmat ovat puutteita järjestelmän suunnittelutasolla. Ensimmäinen ongelma perustuu siihen, kuinka monen vanteen läpi kohteen täytyy hypätä tunnistautuakseen laitteeseen. Puhelimen avaamisprosessi vaatisi käyttäjää 1. avaamaan toisen puhelimen, 2. kirjautumaan siihen, 3. avaamaan identiteettilompakon, 4. hyväksymään tunnistautumisen lompakossa. On haastavaa löytää perusteita näin monimutkaisen menetelmän käyttämiseen, sillä turvallisuustason noususta riippumatta

monimutkaiset ja epäkäytännölliset tunnistautumismenetelmät nähdään tyypillisesti rasittavina käyttäjien kesken [79] [83]. Perustuen todettuun ilmiöön, että esim. määräys salasanojen jaksoittaisesta vaihtamisesta heikentää käyttäjien salasanojen laatua [84], voidaan pitää mahdollisena tai jopa todennäköisenä, että tämän tunnistautumismenetelmän epäkäytännöllisyys ajaisi käyttäjät käyttämään yksinkertaisempia tunnistautumismenetelmiä. Toinen ongelma syntyy siitä, että identiteettilompakkoon pohjautuva ratkaisu luottaa jaettuun identiteettiin, joka on fundamentaalisesti biometristä informaatiota heikompi peruste sähköiselle tai fyysiselle tunnistautumiselle [4]. Esimerkiksi älypuhelimen sormenjälkitunnistin on ratkaisevasti käytännönläheisempi ja teoreettisesti vahvempi tunnistautumismenetelmä kuin tässä kappaleessa esitetty ratkaisu [4][44]. Identiteettilompakkoon perustuva tunnistautuminen sähkölaitteeseen luottaa hyvin kapeaan markkinarakoon, jossa mahdollisimman korkea tunnistautumiskynnys halutaan implementoida ilman biometrisen tunnistautumisen edellyttämiä rakenteellisia ominaisuuksia.

On kuitenkin vähintään yksi konteksti, jossa tämä eurooppalaiseen identiteettilompakkoon perustuva tunnistatutumismenetelmä loistaa. Kyseessä on puhelinvarkaus, jossa kohde menettää puhelimensa varkauden seurauksena. Esim. Google-tilin mahdollistama puhelimen etälukitusominaisuus antaa käyttäjälle mahdollisuuden suojata puhelin lukitusnäytöllä omistajan etänä tekemän pyynnön perusteella [85], jolloin varkaan täytyy rikkoa pyydetty PIN-koodi, kuvio tai salasana tai ohittaa lukitusnäyttö siitä löydetyn haavoittuvuuden perusteella. Jos etälukitusominaisuus mahdollistaa puhelimen lukitusnäytön vaihtamisen etänä, puhelimen omistaja voisi varkaustilanteessa vaihtaa normaalisti käyttämänsä lukitusmenetelmän identiteettilompakkoon perustuvaan menetelmään, jolloin esitetyn järjestelmän sankka turvallisuus/mukavuussuhde toimii esteenä varkaan ja puhelimen sisällön välillä. Olettaen, että eurooppalaiseen identiteettilompakkoon perustuva sähköinen tunnistautumispyyntö on mahdoton murtaa käytännöllisessä ajassa, varas ei pysty avaamaan pu-

helinta ilman lukitukseen sidottua toista puhelinta, jonka päätesovellukseen tunnistautumispyynnöt lähetetään. Tässä kontekstissa esitetty käyttötapaus tarjoaa maksimaalisen turvallisuuden, eivätkä sen haittapuolet haittaa käyttäjää.

## 6.3 Salasanojen korvaaminen

Viimeinen idea uudelle identiteettilompakon käyttötapaukselle on salasanojen korvaaminen identiteettilompakon mukaisella sähköisellä tunnistautumisella. Idea voidaan toteuttaa kahdella tavalla, joista ensimmäinen vaatii palveluntarjoajien tekemiä muutoksia ja toinen ei. Ensimmäisessä ideassa kaikki palveluntarjoajat hyväksyvät lompakkotunnistautumisen palveluihinsa. Idea on utopistinen, sillä lompakkotunnistautuminen on mahdollista ainoastaan palveluissa, jotka hyväksyvät sen käytön, eli jokaisen palvelun täytyy implementoida tunnistautuminen erikseen [30]. Toinen vaihtoehto, joka ei vaadi minkäänlaisia palveluntarjoajien muutoksia, on tietokonesovellus joka palauttaa käyttäjätunnuksen ja salasanan vahvaa sähköistä tunnistautumista vastaan. Käytännössä projektin lopputuote olisi salasanamanageri, johon kirjaudutaan digitaalisella identiteetillä.

Kaksivaiheisella todennuksella varustettuja salasanamanagereita on jo markkinoilla, joten tämä ei ole uusi idea. Esimerkiksi PassCamp [86] suosittelee kaksivaiheista todennusta, jossa manageri pyytää käyttäjää syöttämään satunnaisesti generoidun koodin autentikaatiosovelluksesta kuten Authy tai Google Authenticator [86]. Käytännöllisestä näkökulmasta PassCamp vastaa identiteettilompakkoon perustuvaa manageria. Voidaan sanoa, että idea toimii ainoastaan jos eurooppalainen identiteettilompakko yleistyy tunnistautumismenetelmänä.

# 7 Mielipidekysely eurooppalaisesta identiteettilompakosta

Tämä kysely käsittelee digitaaliseen identiteettiin, kaksivaiheiseen todennukseen ja eurooppalaiseen identiteettilompakkoon liittyviä mielipidekysymyksiä ja väitteitä, joihin kuusi henkilöä ovat antaneet omat vastauksensa. Kysely perustuu aiemmin työssä käsiteltyihin aiheisiin digitaalisen identiteetin nykytilanteesta ja eurooppalaisen identiteettilompakon päätavoitteista. Kysely suoritettiin sessiossa, jossa minä ja kaikki kyselyyn vastaajat olivat samassa huoneessa yhtäaikaisesti. Kyselyn vastaaja vastaa kuhunkin kysymykseen asteikolla 1-5, jotka ilmaisevat vastaajan mielipidettä kyseiseen kysymykseen tai väitteeseen liittyen, tyypillisesti ovatko he samaa vai eri mieltä kysymyksen kanssa. Kyselyn tarkoituksena on kartoittaa vastaanottajien mielipiteitä vahvaan sähköiseen tunnistautumiseen ja sen suunniteltuun kehitykseen liittyen. Kappaleessa esitellään kysely, kyselyn vastaukset sekä tulkitaan vastauksia yksinkertaisia analyyttisiä keinoja hyödyntämällä.

## 7.1 Kysely ja kyselyn vastaukset

Kysely toteutettiin live-tilaisuudessa minun ja vastaajien kesken. Tilaisuudessa esitettiin lyhyt diaesitys, jossa selitettiin identiteetin määritelmä ja rakenne, vahva sähköinen tunnistautuminen, kolmen todentamistekijän tunnistautuminen sekä identiteettilompakon idea kuvan 4.1 mukaisesti. Diaesityksen ansiosta vastaajat ymmär-

sivät aiheen nopeasti. Tilaisuus mahdollisti kyselyn rakenteellisen läpikäynnin, jotta pystyin pysäyttämään vastaajat tiettyihin kysymyksiin ja selittämään tarvittavat taustatiedot. Rakenteellisen läpikäynnin ansiosta pystyin myös vastaamaan ryhmässä esitettyihin kysymyksiin ja ryhmä pystyi keskustelemaan aiheista keskenään. Ryhmäformaatista huolimatta kehotin vastaajia vastaamaan itsenäisesti ja rehellisesti anonymiteetin suojaamana. Läsnäolollani ei missään tapauksessa tähdätty vastausten manipuloimiseen, vastaukset ovat mahdollisimman autenttisia. Autenttisuus on elintärkeää analysoinnin kannalta. Tästä syystä kyselyssä on myös pyritty välttämään sanamuotoja, jotka ohjaisivat vastaajaa positiiviseen tai negatiiviseen tulkintaan. Kysymyksistä on pyritty tekemään mahdollisimman ymmärrettäviä selittämisen tarpeen minimoimiseksi. Tilaisuudessa käydyt keskustelut toivat esille huomioita tiettyihin kysymyksiin. Nämä muistiinpanot huomioidaan ja käsitellään kysymysten ohessa. Kysely tulostettiin paperille vastaustilaisuutta varten. Vastaajat olivat kaksikymppisiä tietotekniikan alan opiskelijoita.

Tässä osiossa esitetään kukin kysymys, vastausvaihtoehdot, vastaukset sekä vastausten keskiarvo ja keskihajonta. Kysymykset jaotellaan kolmeen ryhmään vastausvaihtoehtojen perusteella: lineaarinen asteikko yhdestä viiteen, kyllä/ei- ja monivalintakysymykset. Lisäksi esitetään sanallisia analyysejä vastausten merkityksestä sekä vastaajien tilaisuudessa esille tuomia huomioita.

Taulukko 7.1: Lopputulokset: lineaarinen asteikko
(1: vahvasti eri mieltä - 5: vahvasti samaa mieltä)

| **Kysymys** | **Vastaukset** | **Keskiarvo** | **Keskihajonta** |
|---|---|---|---|
| 1. Epäiletkö koskaan, että "ruudun takana"oleva henkilö ei ole se joka näkyy ruudulla? | 3, 4, 4, 3, 4, 3 | 3,50 | 0,50 |
| 2. Digitaaliset identiteetit ovat mielestäsi päteviä tunnistautumisvälineitä. | 5, 4, 5, 4, 3, 4 | 4,17 | 0,69 |

| Kysymys | Vastaukset | Keskiarvo | Keskihajonta |
|---|---|---|---|
| 3. Digitaalinen henkilöllisyystodistus vastaa paperista henkilöllisyystodistusta. | 2, 4, 4, 4, 5, 4 | 3,83 | 0,90 |
| 4. Pankkitunnuksiin perustuva henkilöllisyyden osoittaminen vastaa henkilökorttia tai passia. | 5, 4, 3, 4, 3, 4 | 3,83 | 0,69 |
| 8. Avainlukulista on viime vuosina korvattu mobiilivarmenteella. Luotatko mobiilivarmenteeseen henkilöllisyyden todentamismenetelmänä? | 4, 5, 5, 3, 3, 5 | 4,17 | 0,90 |
| 10. Onko mobiilivarmenne mielestäsi kömpelö tai epäkäytännöllinen arkipäiväisessä pankkiasioinnissa (avainlukulistaan verrattuna)? | 5, 5, 5, 4, 5, 4 | 4,67 | 0,47 |
| 11. Mobiilivarmenne helpottaa arkipäiväistä pankkiasiointiani. | 5, 5, 5, 5, 5, 5 | 5,00 | 0,00 |
| 14. Pakollinen kaksivaiheinen tunnistautuminen ärsyttää minua. | 2, 1, 2, 1, 2, 1 | 1,50 | 0,50 |
| 16. Pidän ajatuksesta, että yksi tunnistautumisväline sisältää avaimet käyttäjätileihini lukuisissa palveluissa. | 2, 5, 5, 2, 3, 4 | 3,50 | 1,26 |
| 17. Kaksivaiheisen tunnistautumisen lisäämä turvallisuus on sen lisäämän epäkäytännöllisyyden arvoinen. | 5, 5, 5, 4, 5, 5 | 4,83 | 0,37 |
| 18. Vahva sähköinen tunnistautuminen fyysiseen laitteeseen voisi olla hyödyllinen ominaisuus. | 4, 4, 5, 2, 4, 3 | 3,67 | 0,94 |
| 19. Jos puhelimesi varastettaisiin, harkitsisitko puhelimen lukituksen vaihtamista etänä kaksivaiheista todennusta vaativaan tilaan? | 5, 4, 5, 3, 4, 4 | 4,17 | 0,69 |
| 21. Luotan Suomi.fi-verkkotunnistautumiseen. | 5, 4, 5, 4, 4, 5 | 4,50 | 0,50 |
| 26. Suomi.fi-verkkotunnistautuminen on mielestäni liian hidas ja/tai monivaiheinen prosessi. | 2, 3, 3, 2, 1, 1 | 2,00 | 0,82 |
| 27. Vahvan sähköisen tunnistautumisen yhteydessä palveluntarjoaja tulisi valtuuttaa kertomaan täsmälleen mitä attribuutteja palveluntarjoaja lukee identiteetin sisältä. | 5, 5, 5, 5, 5, 5 | 5,00 | 0,00 |
| 28. Kohteen tulisi pystyä määräämään, mitä identiteetin sisältämiä tietoja luovutetaan asiointipalvelun luettavaksi tunnistautumisen yhteydessä. | 5, 3, 5, 4, 5, 4 | 4,33 | 0,75 |

| Kysymys | Vastaukset | Keskiarvo | Keskihajonta |
|---|---|---|---|
| 29. Kohteen tulisi pystyä näkemään historia palveluista, joihin identiteetin sisältämiä tietoja on luovutettu (ja/tai luovutetaan edelleen) sekä mitä tietoa on luovutettu? | 5, 5, 5, 5, 5, 5 | 5,00 | 0,00 |
| 30. Kohteen tulisi pystyä peruuttamaan tietojen luovuttaminen sähköiseen asiointipalveluun/palveluihin omasta tahdostaan. | 5, 5, 5, 4, 5, 4 | 4,67 | 0,47 |
| 31. Lainomaisen huoltajan tulisi pystyä aktivoimaan eurooppalainen identiteettilompakko asianomaisen (esim. vanhuksen) puolesta, jos asianomainen ei itse kykene. | 4, 5, 5, 3, 4, 5 | 4,33 | 0,75 |
| 32. Identiteetintarjoajien tulisi pystyä muokkaamaan identiteettilompakkoihin tallennettua dataa sen valvonnan lisäksi ilman kohteen hyväksyntää. | 1, 1, 3, 2, 1, 2 | 1,67 | 0,75 |
| 33. Identiteetintarjoajien tulisi pystyä muokkaamaan dataa kohteen hyväksynnällä. | 5, 5, 5, 4, 5, 5 | 4,83 | 0,37 |
| 34. Identiteettilompakkokonseptin tulisi olla julkisen hallinnon hallinnassa, ei tekniikkajättien kuten Google tai Meta (=Facebook). | 5, 1, 5, 5, 5, 2 | 3,83 | 1,68 |
| 35. Identiteettilompakko tulisi vähentämään aktiivisten digitaalisten identiteettien monimuotoisuutta ja keskittämään niiden käyttöä yhteen sovellukseen. Onko tämä mielestäsi positiivinen asia? | 3, 4, 4, 4, 2, 4 | 3,50 | 0,76 |
| 36. Vahva sähköinen tunnistautuminen sosiaalisen median palveluun (esim. Facebook ja Twitter) on mielestäni hyvä idea. | 4, 1, 4, 4, 2, 4 | 3,17 | 1,21 |
| 37. Edellisen kysymyksen mukainen sosiaalisen median tunnistautuminen voisi muuttua pakolliseksi esim. lakimuutosten perusteella. Olisiko tämä mielestäsi hyvä idea? | 2, 2, 3, 1, 3, 3 | 2,33 | 0,75 |
| 38. Jätätkö puhelimesi koskaan valvomatta julkisiin paikkoihin (esim. hetkellisesti pöydälle tai tiskille)? | 1, 1, 3, 2, 2, 1 | 1,67 | 0,75 |

Taulukko 7.2: Lopputulokset: kyllä/ei-kysymykset

| Kysymys | Vastaukset | Kyllä (%) | Ei (%) |
|---|---|---|---|
| 6. Oletko käyttänyt pankin avainlukulistaa? | Olen (6), En ole (0) | 100 | 0 |

| Kysymys | Vastaukset | Kyllä (%) | Ei (%) |
|---|---|---|---|
| 7. Käytätkö OP mobiilia, Nordea ID:tä tai muuta vastaavaa pankin mobiilivarmennetta? | Käytän (6), En käytä (0) | 100 | 0 |
| 9. Onko luottamuksesi mobiilivarmenteeseen avainlukulistaa vahvempi? | Kyllä (6), Ei (0) | 100 | 0 |
| 12. Tiedätkö, mitä tarkoitetaan kaksivaiheisella tunnistautumisella? | Tiedän (6), En tiedä (0) | 100 | 0 |
| 15. Pyritkö keskittämään kaksivaiheista tunnistautumistasi yhteen tunnistautumisvälineeseen (esim. Google Authenticator)? | Kyllä (4), Ei (2) | 66,666... | 33,333... |
| 20. Tiedätkö, mitä tarkoitetaan Suomi.fi-verkkotunnistautumisella? | Kyllä (6), Ei (0) | 100 | 0 |
| 22. Tiesitkö, että Digi- ja Väestötietovirasto (DVV) hallitsee ja ylläpitää Suomi.fi-verkkotunnistautumista? | Tiesin (1), En tiennyt (5) | 16,666... | 83,333... |
| 23. Tiesitkö, että Suomi.fi-tunnistautuminen perustuu DVV:n ylläpitämään Finnish Trust Networkkiin (FTN)? | Tiesin (0), En tiennyt (6) | 0 | 100 |
| 24. Tiesitkö, että FTN:n rakenteesta johtuen luottamussuhde kohteen (=sinun) ja DVV:n välillä on epäsuora Suomi.fi-verkkotunnistautumisen aikana? | Tiesin (1), En tiennyt (5) | 16,666... | 83,333... |
| 42. Sulkeutuuko puhelimesi näyttö automaattisesti, kun se on riittävän kauan käyttämättömänä? | Kyllä (6), Ei (0) | 100 | 0 |

Taulukko 7.3: Lopputulokset: monivalintakysymykset

| Kysymys | Vastaukset | 1(%) | 2(%) | 3(%) | 4(%) | 5(%) |
|---|---|---|---|---|---|---|
| 5. (Vapaavalintainen) Pohdi, mitä vahvoja sähköisiä tunnistautumismenetelmiä käytät. | Google Authenticator (5), Nordea ID (4), Microsoft Authenticator (2), OP Mobiili (2), Daske Bank ID (1) | 83,3.. | 66,6.. | 33,3.. | 33,3.. | 16,6.. |

| **Kysymys** | **Vastaukset** | **1(%)** | **2(%)** | **3(%)** | **4(%)** | **5(%)** |
|---|---|---|---|---|---|---|
| 13. Käytätkö kaksivaiheista tunnistautumista sähköisissä palveluissa? | Käytän, aina kun mahdollista (1), Käytän, kun tili on mielestäni arvokas tai suojelemisen arvoinen (5), Käytän, jos palvelu pakottaa (0), En käytä palvelua, jos kaksivaiheinen tunnistautuminen on pakollista (0) | 16,6.. | 83,3.. | 0 | 0 | - |
| 25. Onko luottamuksesi Suomi.fi-verkkotunnistautumiseen muuttunut saamiesi tietojen perusteella? | Kyllä, luottamus kasvaa (3), Kyllä, luottamus heikkenee (0), Ei (2), En tiedä (1) | 50 | 0 | 33,3.. | 16,6.. | - |
| 39. Jos jätät (puhelimen julkisiin paikkoihin), suljetko puhelimen näytön ensin? | Kyllä (3), En (0), En jätä puhelintani julkisiin paikkoihin (3) | 50 | 0 | 50 | - | - |
| 40. Jääkö puhelin edelleen valvomatta jos ruudulla on aukinainen väärinkäytölle altis sovellus (esim. pankin mobiilisovellus)? | Kyllä (useammin) (0), Kyllä (ei vaikuta toimintatapoihin) (0), Kyllä (harvemmin) (1), En jätä puhelintani julkisiin paikkoihin (5) | 0 | 0 | 16,6.. | 83,3.. | - |
| 41. Suljetko näytön, kun laitat puhelimen taskuun? | Kyllä (5), Joskus (1), En (0) | 83,3.. | 16,6.. | 0 | - | - |

### 7.1.1 Kyselyn analysointi ja huomiot

Tässä kappaleessa tuodaan esille sanallisia analyysejä kappaleessa 7.1 esitetyistä vastauksista, sekä miten ne suhtautuvat omiin näkemyksiini aiemmissa kappaleissa esitettyjen tietojen perusteella. Analyysien lisäksi tuodaan esille huomiot, jotka

nousivat esiin live-tilaisuuden aikana ryhmän keskinäisen keskustelemisen seurauksena. Valtaosa taulukossa 7.2 esitetyistä kysymyksistä ovat merkityksettömiä live-tilaisuuden ulkopuolella. Näistä kysymyksistä ei välttämättä voi rakentaa syvällistä analyysiä. Analyysi aloitetaan kysymyksestä yksi ja päätetään kysymykseen 42.

| | | | |
|---|---|---|---|
| 1. Epäiletkö koskaan, että "ruudun takana"oleva henkilö ei ole se joka näkyy ruudulla? | 3, 4, 4, 3, 4, 3 | 3,50 | 0,50 |

Kysymys yksi osoittaa, että otanta suhtautuu varovaisesti arkielämässä näkemiään digitaalisia identiteettejä kohtaan. Vahva sähköinen tunnistautuminen lieventää tätä pelkoa, eli se on yksi keino heidän luottamuksensa vahvistamiseksi.

| | | | |
|---|---|---|---|
| 2. Digitaaliset identiteetit ovat mielestäsi päteviä tunnistautumisvälineitä. | 5, 4, 5, 4, 3, 4 | 4,17 | 0,69 |

Kysymys kaksi vihjaa samaan suuntaan kuin kysymys yksi, sillä vastausten keskiarvon perusteella otanta uskoo, että digitaaliset identiteetit ovat päteviä tunnistautumisvälineitä. Digitaalisen identiteetin käsite on tämän kysymyksen perusteella luotettava, mutta niiden väärinkäyttö askarruttaa.

| | | | |
|---|---|---|---|
| 3. Digitaalinen henkilöllisyystodistus vastaa paperista henkilöllisyystodistusta. | 2, 4, 4, 4, 5, 4 | 3,83 | 0,90 |

Tämä kysymys on täsmällinen evoluutio toisesta kysymyksestä. Mielestäni vastaus tukee ajatusta, että otanta ei erityisesti epäile tai pelkää digitaalisen identiteetin käsitettä, ainoastaan niiden väärinkäyttöä.

| | | | |
|---|---|---|---|
| 4. Pankkitunnuksiin perustuva henkilöllisyyden osoittaminen vastaa henkilökorttia tai passia. | 5, 4, 3, 4, 3, 4 | 3,83 | 0,69 |

Sisällöllisesti kysymys neljä vastaa kysymystä kolme, eli sillä selvitetään loppukäyttäjien ja digitaalisten identiteettien välisen luottamuksen vahvuutta. Näiden kysymysten vastausten perusteella otanta uskoo, että paperiset tunnistamisvälineet ovat luotettavampia kuin digitaaliset, että paperiset ovat "korkeammalla tasolla".

| | | | | | | |
|---|---|---|---|---|---|---|
| 5. (Vapaavalintainen) Pohdi, mitä vahvoja sähköisiä tunnistautumismenetelmiä käytät. | Google Authenticator (5), Nordea ID (4), Microsoft Authenticator (2), OP Mobiili (2), Daske Bank ID (1) | 83,3.. | 66,6.. | 33,3.. | 33,3.. | 16,6.. |

Vastausten perusteella Google Authenticator on erittäin suosittu tunnistamisväline otannan keskuudessa.

| | | | |
|---|---|---|---|
| 6. Oletko käyttänyt pankin avainlukulistaa? | Olen (6), En ole (0) | 100 | 0 |

Tämä on live-tilaisuutta varten kirjoitettu lähtötietokysymys. Kieltävä vastaus johtaa siihen, että selitän vastaajalle, mikä avainlukulista on ja miten se toimii.

| | | | |
|---|---|---|---|
| 7. Käytätkö OP mobiilia, Nordea ID:tä tai muuta vastaavaa pankin mobiilivarmennetta? | Käytän (6), En käytä (0) | 100 | 0 |

Tämäkin on live-tilaisuutta varten kirjoitettu lähtötietokysymys.

| | | | |
|---|---|---|---|
| 8. Avainlukulista on viime vuosina korvattu mobiilivarmenteella. Luotatko mobiilivarmenteeseen henkilöllisyyden todentamismenetelmänä? | 4, 5, 5, 3, 3, 5 | 4,17 | 0,90 |

Tilaisuudessa vahvistettiin, että kysymyksessä tarkoitetaan yleistä luottamusta pankkien tunnuslukusovelluksiin, ei luottamusta avainlukulistaan verrattuna. Vastausten perusteella nämä sovellukset ovat luotettuja tunnistamismenetelmiä.

| | | | |
|---|---|---|---|
| 9. Onko luottamuksesi mobiilivarmenteeseen avainlukulistaa vahvempi? | Kyllä (6), Ei (0) | 100 | 0 |

Yksimielinen positiivinen vastaus tähän kysymykseen on mielestäni loistava lopputulos. Se osoittaa, että paperinen tunnistamismenetelmä voidaan korvata digitaalisella tunnistamismenetelmällä loppukäyttäjän luottamusta kasvattavalla tavalla.

| | | | |
|---|---|---|---|
| 10. Onko mobiilivarmenne mielestäsi kömpelö tai epäkäytännöllinen arkipäiväisessä pankkiasioinnissa (avainlukulistaan verrattuna)? | 5, 5, 5, 4, 5, 4 | 4,67 | 0,47 |

Tämä on käyttäjäkokemuskysymys. 5 tarkoittaa, että avainlukulista on hyvin kömpelö mobiilivarmenteeseen verrattuna. Vastaukset tukevat kappaleen 3.1.1 hypoteesia, että Osuuspankin verkkotunnistaminen on käyttäjäkokemukseltaan positiivinen.

| | | | |
|---|---|---|---|
| 11. Mobiilivarmenne helpottaa arkipäiväistä pankkiasiointiani. | 5, 5, 5, 5, 5, 5 | 5,00 | 0,00 |

Kysymys 11 tukee edellistä kysymystä ja vahvistaa siitä muodostettua tulkintaa.

| | | | |
|---|---|---|---|
| 12. Tiedätkö, mitä tarkoitetaan kaksivaiheisella tunnistautumisella? | Tiedän (6), En tiedä (0) | 100 | 0 |

Tämäkin on lähtötietokysymys, jota ei voi analysoida.

| | | | | | | |
|---|---|---|---|---|---|---|
| 13. Käytätkö kaksivaiheista tunnistautumista sähköisissä palveluissa? | Käytän, aina kun mahdollista (1), Käytän, kun tili on mielestäni arvokas tai suojelemisen arvoinen (5), Käytän, jos palvelu pakottaa (0), En käytä palvelua, jos kaksivaiheinen tunnistautuminen on pakollista (0) | 16,6.. | 83,3.. | 0 | 0 | - |

Mielestäni otannan halukkuus kaksivaiheisten tunnistamismenetelmien käyttämiseen on tärkeää, sillä eurooppalainen identiteettilompakko on sellainen. Toisaalta, jos tili ei ole arvokas, kaksivaiheiselle tunnistautumiselle ei aina ole perustetta.

| | | | |
|---|---|---|---|
| 14. Pakollinen kaksivaiheinen tunnistautuminen ärsyttää minua. | 2, 1, 2, 1, 2, 1 | 1,50 | 0,50 |

Kysymys 14 tukee aiempaa kysymystä. Otanta ei ärsyynny, vaikka palvelu vaatisi kaksivaiheista tunnistautumista, koska he käyttävät sitä pakottamattakin.

| | | | |
|---|---|---|---|
| 15. Pyritkö keskittämään kaksivaiheista tunnistautumistasi yhteen tunnistautumisvälineeseen (esim. Google Authenticator)? | Kyllä (4), Ei (2) | 66,666... | 33,333... |

Mielestäni tähän kysymykseen ei ole oikeaa tai väärää vastausta, kunhan välineet ovat luotettavia. Yhden välineen käyttäminen edistää käyttäjäkokemusta, sillä kaikki avaimet ovat yhdessä sovelluksessa. Usean välineen käyttäminen tuottaa turvallisuusedun, koska yhteen murtautuminen ei mahdollista pääsyä kaikkiin palveluihin.

| | | | |
|---|---|---|---|
| 16. Pidän ajatuksesta, että yksi tunnistautumisväline sisältää avaimet käyttäjätileihini lukuisissa palveluissa. | 2, 5, 5, 2, 3, 4 | 3,50 | 1,26 |

Tämä kysymys iskee edellisen kysymyksen analyysissä esitettyyn periaatteeseen. Vastaukset ovat hyvin jakautuneita ja pääsääntöisesti vastaavat edellisen kysymyksen kyllä/ei-vastauksia. Matalat arvot arvostavat turvallisuutta, suuret mukavuutta.

| | | | |
|---|---|---|---|
| 17. Kaksivaiheisen tunnistautumisen lisäämä turvallisuus on sen lisäämän epäkäytännöllisyyden arvoinen. | 5, 5, 5, 4, 5, 5 | 4,83 | 0,37 |

Kaksivaiheinen tunnistautuminen kasvattaa turvallisuutta käytännöllisyyden kustannuksella [83]. Vastaajat ovat yksimielisesti turvallisuuden puolella, mutta turhan epäkäytännöllisyyden välttäminen on hyödyllistä turvallisuuden edistämisessä [84].

| | | | |
|---|---|---|---|
| 18. Vahva sähköinen tunnistautuminen fyysiseen laitteeseen voisi olla hyödyllinen ominaisuus. | 4, 4, 5, 2, 4, 3 | 3,67 | 0,94 |

Kysymys koskee kappaleessa 6.2 esitettyä ominaisuutta. Selitin miten ominaisuus toimii ennen kysymykseen vastaamista. Ensimmäinen kommentti: ominaisuus voisi toimia paremmin, jos avain olisi kehossa kiinni oleva laite, esim. älykello. Toinen

kommentti: ominaisuus kuulostaa järkevältä, kun puhelin avaa tietokoneen. Kolmas kommentti: tällaisia työkaluja on jo olemassa.

| | | | |
|---|---|---|---|
| 19. Jos puhelimesi varastettaisiin, harkitsisitko puhelimen lukituksen vaihtamista etänä kaksivaiheista todennusta vaativaan tilaan? | 5, 4, 5, 3, 4, 4 | 4,17 | 0,69 |

Kappaleessa 6.2 esitettiin käyttötapaus, jossa omistaja kytkee ominaisuuden päälle varkauden jälkeen epäkäytännöllisyyden välttämiseksi. Näyttää vaikuttavan positiivisesti vastausten keskiarvoon. Kommentti: tällaisia työkaluja on jo olemassa.

| | | | |
|---|---|---|---|
| 20. Tiedätkö, mitä tarkoitetaan Suomi.fi-verkkotunnistautumisella? | Kyllä (6), Ei (0) | 100 | 0 |

Tämä on lähtötietokysymys, jota ei voi analysoida.

| | | | |
|---|---|---|---|
| 21. Luotan Suomi.fi-verkkotunnistautumiseen. | 5, 4, 5, 4, 4, 5 | 4,50 | 0,50 |

Otanta luottaa nykyiseen Suomi.fi-verkkotunnistautumiseen, mikä on mielestäni ymmärrettävää, sillä Suomi.fi-kirjautumista käytetään kaikissa suomen julkihallinnon palveluissa, mukaan lukien Kela ja OmaKanta.

| | | | |
|---|---|---|---|
| 22. Tiesitkö, että Digi- ja Väestötietovirasto (DVV) hallitsee ja ylläpitää Suomi.fi-verkkotunnistautumista? | Tiesin (1), En tiennyt (5) | 16,666... | 83,333... |
| 23. Tiesitkö, että Suomi.fi-tunnistautuminen perustuu DVV:n ylläpitämään Finnish Trust Networkkiin (FTN)? | Tiesin (0), En tiennyt (6) | 0 | 100 |
| 24. Tiesitkö, että FTN:n rakenteesta johtuen luottamussuhde kohteen (=sinun) ja DVV:n välillä on epäsuora Suomi.fi-verkkotunnistautumisen aikana? | Tiesin (1), En tiennyt (5) | 16,666... | 83,333... |

Kysymyksiin 22, 23 ja 24 vastattiin kunkin osanottajan lähtötietojen perusteella. Kysymykset koskevat kappaletta 3. Tietämättömien vastausten valtaisa määrä tuottaa hyvän pohjan kysymykselle 25.

| | | | | | | |
|---|---|---|---|---|---|---|
| 25. Onko luottamuksesi Suomi.fi-verkkotunnistautumiseen muuttunut saamiesi tietojen perusteella? | Kyllä, luottamus kasvaa (3), Kyllä, luottamus heikkenee (0), Ei (2), En tiedä (1) | 50 | 0 | 33,3.. | 16,6.. | - |

Ennen tähän kysymykseen vastaamista selitin kysymysten 22, 23 ja 24 sisällön vastaajille. Selitin, miten FTN:n luottamusverkosto toimii ja miksi loppukäyttäjän ja DVV:n luottamussuhde on epäsuora kappaleen 3 mukaisesti. Vastaajat ilmaisivat luottamussuhteensa muutoksen antamieni tietojen perusteella. Fakta, ettei yksikään vastaaja vastannut kieltävästi, on mielestäni positiivinen lopputulos.

| | | | |
|---|---|---|---|
| 26. Suomi.fi-verkkotunnistautuminen on mielestäni liian hidas ja/tai monivaiheinen prosessi. | 2, 3, 3, 2, 1, 1 | 2,00 | 0,82 |

Tähän kysymykseen vastaaminen on varmasti vaikeaa, jos ei ensin lue ja ymmärrä kappaletta 3.1.1. Perinpohjaisesti läpikäytynä vastaukset saattaisivat muuttua.

| | | | |
|---|---|---|---|
| 27. Vahvan sähköisen tunnistautumisen yhteydessä palveluntarjoaja tulisi valtuuttaa kertomaan täsmälleen mitä attribuutteja palveluntarjoaja lukee identiteetin sisältä. | 5, 5, 5, 5, 5, 5 | 5,00 | 0,00 |

Huomio: kysymyksessä esitetty ominaisuus on jo pakollinen GDPR-asetuksen perusteella [87]. Jos/kun tämä ominaisuus syötetään identiteettilompakkoon, otanta näyttää vastaanottavan sen hyvin positiivisesti.

| | | | |
|---|---|---|---|
| 28. Kohteen tulisi pystyä määräämään, mitä identiteetin sisältämiä tietoja luovutetaan asiointipalvelun luettavaksi tunnistautumisen yhteydessä. | 5, 3, 5, 4, 5, 4 | 4,33 | 0,75 |

Tämä kysymys käsittelee samaa aihetta kuin edellinen, mutta toisestä näkökulmasta, jossa kohde määrää tietojen lukuoikeuden. Tämä vaihtoehto vaikuttaa epäsuositulta edelliseen verrattuna. Tämä saattaa johtua siitä, että kohteen päätäntävalta voi olla ristiriidassa palvelun tarpeen kanssa. Kohde pystyisi myös myöntämään oikeuden tietoihin, joita palvelu ei todellisuudessa tarvitse.

| | | | |
|---|---|---|---|
| 29. Kohteen tulisi pystyä näkemään historia palveluista, joihin identiteetin sisältämiä tietoja on luovutettu (ja/tai luovutetaan edelleen) sekä mitä tietoa on luovutettu? | 5, 5, 5, 5, 5, 5 | 5,00 | 0,00 |

Otannan mukaan tämä olisi loistava identiteettilompakon ominaisuus. Lompakko tallentaisi tiedot siitä, mihin ja mitä tietoa lompakosta on luovutettu ja milloin.

| | | | |
|---|---|---|---|
| 30. Kohteen tulisi pystyä peruuttamaan tietojen luovuttaminen sähköiseen asiointipalveluun/palveluihin omasta tahdostaan. | 5, 5, 5, 4, 5, 4 | 4,67 | 0,47 |

Edellä esitetty historiasivu sisältäisi painikkeen, joka päättää tiedon/tietojen jakamisen kyseisen palvelun kanssa. Tämäkin on otannan kesken suosittu ominaisuus.

| | | | |
|---|---|---|---|
| 31. Lainomaisen huoltajan tulisi pystyä aktivoimaan eurooppalainen identiteettilompakko asianomaisen (esim. vanhuksen) puolesta, jos asianomainen ei itse kykene. | 4, 5, 5, 3, 4, 5 | 4,33 | 0,75 |

Mielestäni tämän kysymyksen lopputulos on yhdentekevä, sillä ominaisuus kuuluu jo identiteettilompakon suunnitelmaan [31]. Otannan positiivinen suhtautuminen ominaisuuteen on rohkaiseva lopputulema.

| | | | |
|---|---|---|---|
| 32. Identiteetintarjoajien tulisi pystyä muokkaamaan identiteettilompakkoihin tallennettua dataa sen valvonnan lisäksi ilman kohteen hyväksyntää. | 1, 1, 3, 2, 1, 2 | 1,67 | 0,75 |

Kysymyksen yhteydessä selitettiin, että esim. virallisen nimen vaihtamisen yhteydessä valtion tulisi pystyä muuttamaan identiteettilompakossa oleva nimi, mutta ominaisuutta voidaan käyttää myös petollisesti esim. lähikaupan kanta-asiakkuusstatuksen kanssa. Ensimmäinen kommentti: vastaus riippuu identiteetintarjoajasta. Toinen kommentti: kohteella on mahdollisuus hyväksyä muutos paikan päällä nimen vaihtamisen yhteydessä. Tämä on hyvin kinkkinen kysymys, joten suurempi vastaajamäärä voisi tuottaa erilaisen vastauksen.

| | | | |
|---|---|---|---|
| 33. Identiteetintarjoajien tulisi pystyä muokkaamaan dataa kohteen hyväksynnällä. | 5, 5, 5, 4, 5, 5 | 4,83 | 0,37 |

Vastaukset muuttuvat dramaattisesti, kun muokkaukset tehdään kohteen hyväksynnän alaisena. Mielestäni tämä tieto on tärkeä ja tuo esille sen, että ainakin jotkut kohteet kaipaavat päätäntävaltaa omien identiteettiensä sisällön ja käytön suhteen.

| | | | |
|---|---|---|---|
| 34. Identiteettilompakkokonseptin tulisi olla julkisen hallinnon hallinnassa, ei tekniikkajättien kuten Google tai Meta (=Facebook). | 5, 1, 5, 5, 5, 2 | 3,83 | 1,68 |

Tämän kysymyksen keskihajonta on kaikkia muita suurempi. Kysymys on hyvin polarisoiva, koska siinä puntaroidaan vastaajan luottamusta kahteen laitokseen. Ainoa varma tulkinta on se, ettei kyselyn otanta riitä vastaamaan tähän kysymykseen.

| | | | |
|---|---|---|---|
| 35. Identiteettilompakko tulisi vähentämään aktiivisten digitaalisten identiteettien monimuotoisuutta ja keskittämään niiden käyttöä yhteen sovellukseen. Onko tämä mielestäsi positiivinen asia? | 3, 4, 4, 4, 2, 4 | 3,50 | 0,76 |

Kysymyksellä haetaan takaa ajatusta, että kaikki digitaaliset identiteetit voisivat "vaeltaa"identiteettilompakkoon ajan kuluessa. Vastaaja ennustaa, onko tämä kehityssuunta hyvä vai huono. Huomioiden myös kysymyksistä 15 ja 16 saadut vastaukset, otannan mielipiteet ovat hyvin jakautuneita tässä aihepiirissä.

| | | | |
|---|---|---|---|
| 36. Vahva sähköinen tunnistautuminen sosiaalisen median palveluun (esim. Facebook ja Twitter) on mielestäni hyvä idea. | 4, 1, 4, 4, 2, 4 | 3,17 | 1,21 |

Kysymys koskee kappaleessa 6.1 esitettyä ideaa sosiaalisen median superkirjautumisesta. Yksi huomio: voitaisiin rakentaa kokonaan uusi palvelu, jossa ominaisuus on pakollinen. Ominaisuudessa on selkeästi vahvuuksia ja heikkouksia jotka johtavat jakautuneisiin vastauksiin otannan kesken.

| | | | |
|---|---|---|---|
| 37. Edellisen kysymyksen mukainen sosiaalisen median tunnistautuminen voisi muuttua pakolliseksi esim. lakimuutosten perusteella. Olisiko tämä mielestäsi hyvä idea? | 2, 2, 3, 1, 3, 3 | 2,33 | 0,75 |

Vastausten keskiarvo heikentyy, kun kappaleen 6.1 mukainen ominaisuus esitetään pakollisena. Sen turvallisuus/epäkäytännöllisyyssuhde saattaa olla liian matala [83].

| | | | |
|---|---|---|---|
| 38. Jätätkö puhelimesi koskaan valvomatta julkisiin paikkoihin (esim. hetkellisesti pöydälle tai tiskille)? | 1, 1, 3, 2, 2, 1 | 1,67 | 0,75 |

Kysymykset 38-42 koskevat puhelimen käyttötottumuksia. Näillä kysymyksillä kartoitetaan kappaleessa 6.1 esitettyjä mekanismeja, joilla välttää vahvasti sähköisesti tunnistautuneiden sessioiden joutumista vääriin käsiin. Tämän kysymyksen perusteella otanta pitää puhelimistaan huolta, eli he itse kasvattavat niiden turvallisuutta.

| | | | | | | |
|---|---|---|---|---|---|---|
| 39. Jos jätät (puhelimen julkisiin paikkoihin), suljetko puhelimen näytön ensin? | Kyllä (3), En (0), En jätä puhelintani julkisiin paikkoihin (3) | 50 | 0 | 50 | - | - |

Jos vastaajat sulkevat puhelimensa ennen erkaantumista, vahvasti sisäänkirjautunut sessio voidaan päättää ruudun sulkemishetkellä. Näiden vastausten perusteella tämä mekanismi toimisi tässä ryhmässä.

| | | | | | | |
|---|---|---|---|---|---|---|
| 40. Jääkö puhelin edelleen valvomatta jos ruudulla on aukinainen väärinkäytölle altis sovellus (esim. pankin mobiilisovellus)? | Kyllä (useammin) (0), Kyllä (ei vaikuta toimintatapoihin) (0), Kyllä (harvemmin) (1), En jätä puhelintani julkisiin paikkoihin (5) | 0 | 0 | 16,6.. | 83,3.. | - |

Evoluutio edellisestä kysymyksestä, jonka vastaukset jatkavat kysymyksen 38 muodostamaa suuntaa. Tämä on hyvin hypoteettinen kysymys jonka vastaukset eivät

aina vastaa todellisuutta, koska vastaajan arvio siitä mitä hän tekisi hypoteettisessa tilanteessa on ainoastaan arvio. Toiseksi, tässä kysymyksessä pitäisi olla vastausvaihtoehto "En jätä puhelinta valvomatta tässä tapauksessa".

| | | | | | | |
|---|---|---|---|---|---|---|
| 41. Suljetko näytön, kun laitat puhelimen taskuun? | Kyllä (5), Joskus (1), En (0) | 83,3.. | 16,6.. | 0 | - | - |

Tämä kysymys tähtää täsmällisesti ilmiöön, jossa omistajan taskussa auki oleva puhelin soittelee toisille ihmisille [78]. Vaikuttaa erittäin harvinaiselta tässä ryhmässä.

| | | | |
|---|---|---|---|
| 42. Sulkeutuuko puhelimesi näyttö automaattisesti, kun se on riittävän kauan käyttämättömänä? | Kyllä (6), Ei (0) | 100 | 0 |

Tämä saattaa olla vakio-ominaisuus nykyaikaisissa puhelimissa. Vastausten perusteella mekanismi, joka päättää vahvasti sisäänkirjautuneen session kun näyttö sammuu, toimisi myös tässä kontekstissa. Muut vastaajaryhmät voisivat vastata tähän negatiivisesti.

### 7.1.2 Kyselyn lopputulema

Kaikki kyselyn vastaukset huomioon ottaen vastaukset ovat mielestäni positiivisia, sillä ne ovat vahvasti samassa linjassa eurooppalaisen identiteettilompakon tavoitteiden kanssa [31] [30]. Eritysesti kysymykset, jotka kohdistuvat täsmällisesti lompakon suunniteltuihin ominaisuuksiin, kuten kysymys 31, keräsivät euroopan unionin kannan mukaisia vastauksia hyvin yksimielisesti tässä otannassa. Vastauksien perusteella voidaan todeta, että tietoturva on vastaajille tärkeä periaate eivätkä he luota sokeasti erilaisten järjestelmien ja organisaatioiden tietoturvaan. Tämä väite perustuu erityisesti kysymysten 1, 13, 16, 27, 32, 33 ja 38 vastauksiin. Muut vastaajaryhmät voisivat antaa hyvin erilaisia vastauksia erityisesti kyselyn alussa ja lopussa esitettyihin käyttäjätottumukseen liittyviin kysymyksiin. Tämän tutkimuksen vastaajaryhmä on liian pieni konkreettisten johtopäätösten tekemiseksi, mutta

vastaukset ovat mielestäni rohkaisevia identiteettilompakkoprojektin näkökulmasta. Kysymykset, jotka käsittelevät kappaleessa 6 esitettyjä käyttötapauksia, keräsivät pääosin itseni kanssa samassa linjassa olevia vastauksia tässä ryhmässä. Vastaajat näkivät ominaisuudet positiivisessa valossa ja ehdottivat niihin muutoksia, jotka voisivat johtaa parempaan käyttäjäkokemukseen. Yleisesti katsoen olen tyypillisesti samaa mieltä kyselyn vastausten kanssa.

# 8 Yhteenveto

Vahva sähköinen tunnistautuminen on kehittyvä ala, jonka kehityssuunta on määritetty eurooppalaisen identiteettilompakon suuntaiseksi tämän projektin sisällä. Jos kaikki aiemmissa kappaleissa läpikäydyt aihepiirit tiivistettäisiin yhteen koko työn sisällyttävään kysymykseen, se saattaisi kuulua seuraavasti: "Onko eurooppalainen identiteettilompakko järkevä kehityssuunta vahvan sähköisen tunnistamisen alalle?". Työn perusteella tämän pohdinnan ei pitäisi alkaa näin pinnallisesta kysymyksestä, sillä koko projektin investointi ei olisi koskaan alkanut jos ratkaisussa ei oltaisi nähty suurta potentiaalia. Pohdinnan tulisi alkaa seuraavasta kysymyksestä: "*Miksi* eurooppalainen identiteettilompakko on järkevä kehityssuunta vahvan sähköisen tunnistamisen alalle?". Kysymys on syvällinen, koska se tuo esiin syyt, joilla tämä väite voidaan perustella. Kukin kappale vastaa tähän kysymykseen omalla tavallaan ja kukin kappale tuo esille oman osuutensa tästä vastauksesta. Esimerkiksi kappale 2 esittää säännöt ja periaatteet (digitaalisen) identiteetin koostumukselle ja toiminnalle, joita myös identiteettilompakon täytyy noudattaa ja kappale 3 esittelee nykyaikaisen Finnish Trust Networkin mukaisen tunnistautumisen ja tunnistaa sen sisältämät käyttäjäkokemus- ja atomisaatio-ongelmat. Kaiken kaikkiaan seuraavat argumentit perustelevat miksi eurooppalaista identiteettilompakkoa voidaan pitää arvokkaana tavoitteena:

1. Identiteettilompakkosovelluksen avulla loppukäyttäjälle voidaan tarjota keskitetyt keinot ja valtuudet oman digitaalisen identiteetin ja sen sisältämän

informaation hallitsemiseen [53]. Ks. kappale 5.

2. Identiteettilompakkosovelluksesta pyydetyn datan lukeminen ei anna mahdollisuutta muun identiteetissä olevan datan lukemiseen, jos siihen ei ole myönnetty oikeutta. Asia on toisin paperisissa todistuksissa, joiden kaikki tiedot ovat aina nähtävissä [6].

3. Identiteettilompakko mahdollistaa suoran luottamussuhteen muodostumisen loppukäyttäjän ja tunnistautumismenetelmän välille, joka on nykyisessä FTN-järjestelmässä fundamentaalisesti epäsuora. Ks. kappale 3.1.1.

4. Yhtenäinen identiteettilompakko yhtenäistää identiteetinhallintaa identiteettilompakkoon syötettyjen sähköisten tilien välillä [23]. Ks. kappale 2.2.

5. Identiteettilompakon mukainen tunnistautumisprosessi on FTN:n mukaista käytännönläheisempi. Ks. kappale 3.1.1 ja kuva 4.1.

6. Identiteettilompakkosovelluksella mahdollistetaan uusi mekanismi sähköisten allekirjoitusten luomiseen, hallinnoimiseen ja verifiointiin [30]. Ks. kappale 4.4.

7. Eurooppalaisen identiteettilompakon rakenne vähentää vahvan sähköisen tunnistautumisen alan atomisaatiota. Ks. kappale 3.1.2.

8. Eurooppalaisella identiteettilompakolla voidaan tarjota yhtenäinen EU:n jäsenmaiden välinen menetelmä digitaalisten identiteettien luomiseen, tallentamiseen ja hyötykäyttöön [30].

9. Identiteettilompakon avulla voidaan vähentää yksityisiltä palveluntarjoajilta vaaditun työn määrää omien asiakkaidensa tunnistamisessa. Ks. kappale 6.1.

10. Eurooppalainen identiteettilompakko on vahvan sähköisen tunnistamisen ratkaisu, jonka jäsenvaltio voi itsenäisesti tarjota kaikille kansalaisilleen [30]. Ks. kappale 4.

11. Eurooppalaisen identiteettilompakon olemassaolo voisi potentiaalisesti estää konseptin siirtymisen suurten tekniikkajättien käsiin. EU:n komissiossa painotetaan tämän hierarkiakysymyksen tärkeyttä. [30]. Ks. kappale 4.3.

12. Jokainen Finnish Trust Networkin mukainen tunnistautuminen kustantaa tunnistautumismaksun palveluntarjoajalta [43], identiteettilompakon mukainen ei.

13. Työn yhteydessä pidetty kysely tuotti pääasiallisesti työn muiden kappaleiden näkemysten mukaisia lopputuloksia. Ks. kappale 7.

14. Eurooppalaisen identiteettilompakolla ei ole välitöntä tarvetta nykyaikaisten vahvojen sähköisien tunnistautumismenetelmien korvaamiseen, eli sen käyttöönotto voidaan suorittaa osittaisesti ajan kuluessa [30].

## 8.1 Tutkimuskysymysten vastaukset

Työssä on neljä tutkimuskysymystä, joiden voidaan vastata yksi kerrallaan aiemmissa kappaleissa esitettyjen tietojen perusteella.

1. Miksi tarvitaan digitaalinen identiteetinhallinta- ja lompakko-ohjelmisto?

Edellisen kappaleen neljätoista syytä siihen, miksi identiteettilompakko on järkevä kehityssuunta vahvan sähköisen tunnistamisen alalle, tuottavat vastauksen tähän kysymykseen. Digitaalinen identiteettilompakkoohjelmisto tarvitaan siksi, että se mahdollistaa nykyaikaista käytännöllisemmän, turvallisemman ja yhtenäisen rakenteen vahvalle sähköiselle tunnistautumiselle koko Euroopan unionin alueella [30]. Ohjelmiston käyttöönotto voidaan perustella todella monella tavalla sekä implisiittisesti että eksplisiittisesti siihen sisältyvien ominaisuuksien perusteella.

2. Mitkä tekijät täytyy huomioida, että ohjelmiston käyttäjäkokemus voidaan kehittää nykyratkaisuja paremmaksi?

Tähän kysymykseen vastataan erityisesti kappaleessa 3.1.1, jossa nykyisen Finnish Trust Network (FTN)-järjestelmän käyttäjäkokemushaasteet esitetään, sekä kuvissa 3.1, 3.2 ja 4.1, jotka kuvaavat tunnistautumisprosessia loppukäyttäjän näkökulmasta nykyisillä sekä uudella järjestelmällä. Myös kappaleessa 3.1.2 esitettyä atomisaatio-ongelmaa voidaan tulkita siitä näkökulmasta, että kaikkien FTN:ään kuuluvien tunnistautumismenelmien käyttäjäkokemus eroaa toisistaan [34], mikä johtaa siihen, että käyttäjän täytyy opetella käyttämään kutakin erikseen. Ytimekkäästi sanottuna identiteettilompakon käyttäjäkokemusta voidaan edistää tekemällä siitä yksinkertainen, ymmärrettävä, nopea ja helppokäyttöinen loppukäyttäjän näkökulmasta, sillä FTN ei hyödynnä kaikkia näitä pylväitä [39].

3. Miten ohjelmisto julkaistaan nykyisten ratkaisujen ohelle siten, että siihen siirtyminen hyödyttää loppukäyttäjää?

Eurooppalainen identiteettilompakko tultaisiin hyödyntämään Suomi.fi-palvelussa nykyisin käytetyn Finnish Trust Network (FTN)-järjestelmän [40] sijaan tai yhtenä tunnistautumisvaihtoehtona FTN:n ohella [31]. Edellisessä kappaleessa on esitetty neljätoistakohtainen lista syitä siihen, miksi identiteettilompakko on järkevä kehityssuunta vahvan sähköisen tunnistautumisen alalle. Tämä lista vastaa kysymyksen loppuosaan. Tämän listan lisäksi osa työn ohessa suoritetun kyselyn (ks. kappale 7) kysymyksistä tuovat esiin merkittäviä ominaisuuksia, jotka edistäisivät loppukäyttäjän kykyä hallita omia sähköisiä identiteettejään sekä niiden käyttöä entistäkin tehokkaammin. Ks. taulukon 7.1 kysymykset 18 ja 29 ja kappale 6.2.

4. Miten yksi identiteetinhallintasovellus kattaa sille olennaiset käyttötapaukset? Voidaanko keksiä uusia käyttötapauksia?

Eurooppalainen identiteettilompakko on järjestelmä, johon voidaan tallentaa yksi tai useampi sähköinen tili, joilla voidaan tunnistautua sähköisiin palveluihin eIDAS High-tason vahvalla sähköisellä tunnistautumisella, sillä oletuksella että loppu-

käyttäjä on Euroopan unionin jäsenmaan kansalainen [30] [31]. Tämä kattaa ohjelmistolle olennaiset kriteerit ja mahdollistaa käyttötapaukset. Uusien käyttötapausten keksiminen on mahdollista, ks. kappale 6. Eurooppalaisen identiteettilompakon hyödyntäminen näissä käyttötapauksissa on mahdollista.

## 8.2 Päätelmät

Tässä työssä tehdyn kirjallisen ja empiirisen tutkimuksen perusteella eurooppalainen identiteettilompakko onnistuu omissa päätavoitteissaan ja pystyy myös vastaamaan työn alussa esitettyjen tutkimuskysymysten muodostamaan tarpeeseen. Kirjallisen tutkimuksen perusteella eurooppalainen identiteettilompakko pystyy korjaamaan Finnish Trust Network-järjestelmässä olevia käyttäjäkokemus- ja atomisaatioongelmia (ks. kappaleet 3.1.1 ja 3.1.2). Kappaleessa 7 esitetyn kyselyn analysoinnin perusteella vastaajat, eli potentiaaliset loppukäyttäjät, suhtautuvat identiteettilompakon ominaisuuksiin positiivisesti. Muun muassa lähteisiin [53], [70], [51], [55] ja [54] perustuvan kirjallisen tutkimuksen perusteella kappaleessa 5 esitetty Starwindow® Identiteettilompakko pystyy vastaamaan lompakkosovelluksen raamien esittämiin tarpeisiin teknologian käytännön sovellutuksena. Jatkotutkimuksia ajatellen kappaleessa 7 esitetyn kyselyn otanta rajoittuu ainoastaan kuuteen ihmiseen, joten vastaavien kysymysten esittäminen suuremmalle ihmismäärälle tulee johtamaan akateemisesti hyödylliseen lopputulokseen.

# Lähdeluettelo


[1] H. W. Noonan, *Personal Identity*, 3. painos. Routledge, 2019, ISBN: 9781315107240.

[2] J. E.CÔTÉf1SETH ja J.SCHWARTZ, "Comparing psychological and sociological approaches to identity: identity status, identity capital, and the individualization process", *Journal of Adolescence*, Elsevier Ltd. Vol. 25, nro 6, s. 571–586, 2002.

[3] K. Deaux, "Social identification", *E. T. Higgins A. W. Kruglanski (Eds.), Social psychology: Handbook of basic principles*, The Guilford Press, s. 777–798, 1996.

[4] J. Silander, "Katsaus identiteetinhallinnan teknologioihin ja niiden tulevaisuuden näkymiin", Aalto-yliopisto, Department of Communications and Networking Tietoliikenne- ja tietoverkkotekniikan laitos, 2013.

[5] V. Bruce ja A. W. Young, *Face perception*, 1. painos. Psychology Press, 2012, ISBN: 1841698784.

[6] Poliisi, *Hae henkilökorttia*, `https://poliisi.fi/henkilokortti`, Accessed: 2021-08-30.

[7] G. B. Ayed, "Digital Identity Metadata Scheme: A Technical Approach to Reduce Digital Identity Risks", *2011 IEEE Workshops of International Conference on Advanced Information Networking and Applications*, IEEE, s. 607–612, 2011, Accessed: 2022-06-05.

[8] P. Beynon-Davies, "A survey of new trends in symbolic execution for software testing and analysis", *Information Polity*, Cardiff Business School, Cardiff University, UK, vol. 11, nro 1, s. 3–19, 2006.

[9] jumio, *What is a Digital Identity?*, https://www.jumio.com/what-is-a-digital-identity/, Accessed: 2022-06-16.

[10] C. Wells, Y. Zhang, J. Lukito ja J. C. W. Pevehouse, "Modeling the Formation of Attentive Publics in Social Media: The Case of Donald Trump", *Mass Communication and Society*, DOI, vol. 23, nro 2, s. 181–205, 2018.

[11] *Canon U.S.A., Inc.* https://www.usa.canon.com/, Accessed: 2021-08-30.

[12] Fraud Squad TV Inc., *A Case of Stolen Identity | Scammed | Real Crime*, https://youtu.be/1YcyXLyq8Mk, Accessed: 2021-08-31, 2011.

[13] B. Nelson, *Here's What Hackers Can Do with Just Your Email Address*, https://www.rd.com/list/what-hackers-can-do-with-email-address/, Accessed: 2022-06-16, Reader's Digest.

[14] L. Emanuel ja D. S. Fraser, "Exploring physical and digital identity with a teenage cohort", *IDC '14: Proceedings of the 2014 conference on Interaction design and children*, DOI, s. 67–76, 2014.

[15] A. Greenberg, *HBGary Federal's Aaron Barr Resigns After Anonymous Hack Scandal*, https://www.forbes.com/sites/andygreenberg/2011/02/28/hbgary-federals-aaron-barr-resigns-after-anonymous-hack-scandal/, Accessed: 2022-06-17, Forbes.

[16] C. Stewart III, "Voter ID: Who has them? Who shows them?", *Symposium: Legislative Issues in Election Law*, Oklahoma Law Review, vol. 66, nro 1, 2013, Accessed: 2022-09-18.

[17] S. Bharadwaj, M. Vatsa ja R. Singh, "Biometric quality: a review of fingerprint, iris, and face", *Bharadwaj et al. EURASIP Journal on Image and Video Processing*, SpringerOpen, 2014.

[18] S. Pan, N. Wang, Y. Qian, I. Velibeyoglu, H. Y. Noh ja P. Zhang, "Indoor Person Identification through Footstep Induced Structural Vibration", *IDC '14: Proceedings of the 2014 conference on Interaction design and children*, ACM Digital Library, s. 81–86, 2015.

[19] M. Singh, R. Singh ja A. Ross, "A comprehensive overview of biometric fusion", *Information Fusion*, Elsevier, vol. 52, s. 187–205, 2019.

[20] P. Gupta, S. Behera, M. Vatsa ja R. Singh, "On Iris Spoofing Using Print Attack", *International Conference on Pattern Recognition*, IEEE, vol. 22, s. 1681–1686, 2014.

[21] G. Mingels, *World Population: From Pyramids to Skyscrapers*, `https://www.statista.com/chart/10366/age-structure-of-world-population/`, Accessed: 2021-10-08, DER SPIEGEL/Statista, 2017.

[22] Telecommunication Standardization Sector of ITU, "ITU-T Y.2720. NGN identity management framework", International Telecommunication Union, 2009.

[23] E. Bertino ja K. Takahashi, *Identity Management, Concepts, Technologies, and Systems*. Artech House Publishers, 2011, ISBN: 9781608070398.

[24] I. A. Mohammed, "Systematic Review of Identity Access Management in Information Security", *International Journal of Innovations in Engineering Research and Technology*, Researchgate, vol. 4.7, s. 1–7, 2017, Accessed: 2022-06-23.

[25] N. F. Trust, *What is personal identifiable data*, `https://www.esneft.nhs.uk/about-us/privacy/what-is-personal-identifiable-data/`, Accessed: 2022-11-07.

[26] U. D. of Labor, *Guidance on the Protection of Personal Identifiable Information*, https://www.dol.gov/general/ppii, Accessed: 2022-11-07.

[27] D. ja väestötietovirasto (DVV), *SIOPv2 POC - Guide for Relying Parties - Attributes*, https://wiki.dvv.fi/display/DHHJD/SIOPv2+POC+-+Guide+for+Relying+Parties#SIOPv2POCGuideforRelyingParties-Attributes, Accessed: 2022-11-02, 2022.

[28] Superstore, *How to Prevent Employees from Sharing Access Cards*, https://www.idsuperstore.com/learning-center/how-to-prevent-employees-from-sharing-access-cards/, Accessed: 2022-06-23.

[29] Electronic Frontier Foundation (EFF), *Iris Recognition*, https://www.eff.org/pages/iris-recognition, Accessed: 2022-06-23.

[30] Digi- ja Väestötietovirasto, *VM LIVE 20210916*, https://vimeo.com/606443710/9d76b6b3f4, Accessed: 2021-10-09, 2021.

[31] Digi- ja Väestötietovirasto, *Digital identity program, Request for information, DVV/3873/2020*, https://www.hankintailmoitukset.fi/fi/public/procurement/37528/notice/48723/overview, Document no longer publicly available due to project deadline., 2020.

[32] *OP-verkkopalvelu op.fi*, https://www.op.fi/etusivu, Accessed: 2021-10-20.

[33] European Commission, *Discover eIDAS*, https://digital-strategy.ec.europa.eu/en/policies/discover-eidas, Accessed: 2022-06-29.

[34] *Kela*, https://www.kela.fi/, Accessed: 2021-10-20.

[35] P. Paastela, "Asiakkaan tunnistaminen Tullin asiointipalveluissa", Haaga-Helia ammattikorkeakoulu Oy, Tietojärjestelmäosaamisen koulutusohjelma, 2020.

[36] CEF Digital, *eIDAS Levels of Assurance*, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Levels+of+Assurance, Accessed: 2021-10-13.

[37] Liikenne ja viestintävirasto Traficom - Kyberturvallisuuskeskus, *Tunnistuspalvelurekisteri*, https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tunnistuspalvelurekisteri_18062021.XLSX, Accessed: 2021-10-13.

[38] LuxTrust, *Understanding eIDAS e-signature levels and their associated legal value*, https://www.luxtrust.com/en/news/understanding-eidas-e-signature-levels-and-their-associated-legal-value, Accessed: 2022-06-29, 2019.

[39] P. Stenius, *What is the Finnish Trust Network (FTN)?*, https://www.ubisecure.com/authentication/finnish-trust-network-ftn/, Accessed: 2021-12-02, Ubisecure, 2019.

[40] J. Jellema, *Why use the FTN – Finnish Trust Network?*, https://www.ubisecure.com/identity-provider/why-use-the-ftn-finnish-trust-network/, Accessed: 2021-12-02, Ubisecure, 2019.

[41] Liikenne ja viestintävirasto Traficom - Kyberturvallisuuskeskus, *Sähköinen tunnistaminen*, https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen, Accessed: 2021-10-20.

[42] Digi- ja väestötietovirasto, *Suomi.fi-info 8.6.2022 Info alkaa klo 9.00*, https://dvv.fi/documents/16079645/105542937/06_Suomi.fi-info,+kesakuu+2022,+pdf.pdf/5035e49b-b4a4-071a-b23f-05b99796118b/06_Suomi.fi-info,+kesakuu+2022,+pdf.pdf?version=1.0&t=1654609137492, Accessed: 2022-07-04.

[43] A. Parviala, *Pankki niisti joka verkkotunnistautumisesta jopa 50 senttiä – tänään hinta laskee, mutta otetaanko sentit sinulta? - Yle Uutiset*, https://yle.fi/uutiset/3-9587886, Accessed: 2021-10-27, 2017.

[44] Thales DIS, *Three-factor authentication: Something you know, something you have, something you are*, https://dis-blog.thalesgroup.com/security/2011/09/05/three-factor-authentication-something-you-know-something-you-have-something-you-are/, Accessed: 2021-10-20, 2018.

[45] Corrosionpedia, *Atomization*, https://www.corrosionpedia.com/definition/120/atomization, Accessed: 2021-10-21, 2019.

[46] J. Rahkonen, "Toivo ja yhteisöllisyys 2020-luvulla", *Yhteiskuntapolitiikka*, Julkari, vol. 84, s. 629–634, 2019.

[47] National Geographic, *Nile River*, https://www.nationalgeographic.org/encyclopedia/nile-river/, Accessed: 2021-10-21.

[48] A. Shaikh, *Capitalism, Competition, Conflict, Crises*. Oxford University Press, 2016, Accessed: 2021-12-10, ISBN: 9780199390632.

[49] ReportLinker, *The global e-signature market is expected to advance at a CAGR of 26.6% from 2021 to 2030 (forecast period) and reach $12,721.4 million revenue by 2030*, https://www.globenewswire.com/news-release/2021/08/18/2282584/0/en/The-global-e-signature-market-is-expected-to-advance-at-a-CAGR-of-26-6-from-2021-to-2030-forecast-period-and-reach-12-721-4-million-revenue-by-2030.html, Accessed: 2021-11-15, 2021.

[50] Adobe, *What is a digital signature  how does it work | Adobe Sign*, https://www.adobe.com/sign/digital-signatures.html, Accessed: 2022-02-24.

[51] *Electronic signature REST API*, Yksityinen, Gurulogic Microsystems Oy.

[52] E. Pagano, *Mikä on julkisen avaimen salaustekniikka?*, https://www.ssl.com/fi/FAQ/mikä-on-julkisen-avaimen-salaustekniikka/, Accessed: 2022-09-08, SSL.com, 2019.

[53] *Starwindow® KeyStore - Introduction in brief*, Yksityinen, Gurulogic Microsystems Oy.

[54] *SWKS Palvelukuvaus*, Yksityinen, Gurulogic Microsystems Oy.

[55] *Käyttäjätietojen käsittelyn hallinta: Holvipalvelu*, Yksityinen, Gurulogic Microsystems Oy.

[56] *SP UC7.1 Attribuuttitodistus puhelinnumerolla*, Yksityinen, Gurulogic Microsystems Oy.

[57] European Commission EUDIW Toolbox Group, *European Digital Identity Architecture and Reference Framework Outline*, `https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline`, Accessed: 2022-12-02, 2022.

[58] *Tunnistautuminen passilla*, Yksityinen, Gurulogic Microsystems Oy.

[59] *Pankkitunnistautuminen*, Yksityinen, Gurulogic Microsystems Oy.

[60] Cámara de Comercio de Bogotá, *What are the differences between a natural and a legal person?*, `https://www.ccb.org.co/en/Frequently-Asked-Questions/Registration-processings/What-are-the-differences-between-a-natural-and-a-legal-person`, Accessed: 2022-12-02.

[61] NFCRead, *MRZ / MACHINE READABLE ZONE*, `https://www.nfcread.com/en/mrz-info-machine-readable-zone`, Accessed: 2022-12-17.

[62] *SRIS Käsitemalli*, Yksityinen, Gurulogic Microsystems Oy.

[63] Amazon Web Services (AWS), *The key-value database defined*, `https://aws.amazon.com/nosql/key-value/`, Accessed: 2022-11-30, 2022.

[64] Tracy V. Wilson, *How Broadcast Messaging Works*, `https://computer.howstuffworks.com/e-mail-messaging/broadcast-messaging.htm`, Accessed: 2022-11-30, HowStuffWorks, 2022.

[65] J. O. Dhruv Mohindra, *SER02-J. Sign then seal objects before sending them outside a trust boundary*, https://wiki.sei.cmu.edu/confluence/display/java/SER02-J.+Sign+then+seal+objects+before+sending+them+outside+a+trust+boundary, Accessed: 2022-11-30, Carnegie Mellon University, Software Engineering Institute, 2021.

[66] *SP UC5.3 Vault-palveluiden linkitys*, Yksityinen, Gurulogic Microsystems Oy.

[67] *Starwindow® LinkVault-teknologia*, Yksityinen, Gurulogic Microsystems Oy.

[68] Gurulogic Microsystems Oy, *Methods and arrangements for establishing digital identity (EP22157019.5)*, Ei vielä julkisesti saatavilla, jätetty 16.02.2022. European Patent Office.

[69] T. Kärkkäinen, O. Kalevo ja M. Sahlbom, *Protecting Usage of Key Store Content*, https://gurulogic.com/files/patents/EP3549304B1.pdf, Accessed: 2022-09-16, European Patent Office, 2020.

[70] *Starwindow® Vault Service*, Yksityinen, Gurulogic Microsystems Oy.

[71] T. M. Kärkkäinen, *System and method for providing protected data storage in a data memory*, https://gurulogic.com/files/patents/GB2576755B.pdf, Accessed: 2022-09-16, European Patent Office, 2021.

[72] Twitter Help Center, *About Verified Accounts*, https://help.twitter.com/en/managing-your-account/about-twitter-verified-accounts, Accessed: 2021-11-05.

[73] N. Zhou, *Twitter hacked: panic and joy as verified users with blue tick forbidden from posting*, https://www.theguardian.com/technology/2020/jul/16/twitter-hacked-panic-and-joy-as-verified-users-with-blue-tick-forbidden-from-posting, Accessed: 2021-11-10, The Guardian.

[74] Reuters, *Elon Musk updates Twitter app to start charging $8 for blue checkmark*, https://www.dawn.com/news/1719362/elon-musk-updates-twitter-app-to-start-charging-8-for-blue-checkmark, Accessed: 2022-11-06, 2022.

[75] redisson, *What is a Web Session?*, https://redisson.org/glossary/web-session.html, Accessed: 2022-03-13.

[76] Lookout, *Phone theft in America, Breaking down the phone theft epidemic*, https://transition.fcc.gov/cgb/events/Lookout-phone-theft-in-america.pdf, Accessed: 2022-03-15, Federal Communications Commission (FCC), 2014.

[77] a.p.i alarm inc., *How Long Does the Average Burglary Last*, https://www.apialarm.com/blog/protection/how-long-does-the-average-burglary-last/, Accessed: 2022-03-15.

[78] W. Gordon, *How to Stop Butt Dialing Everyone with Your Smartphone*, https://www.wired.com/story/stop-pocket-butt-dialing/, Accessed: 2022-03-15, Wired, 2020.

[79] J.-E. R. Lee, S. Rao, C. Nass, K. Forssell ja J. M. John, "When do online shoppers appreciate security enhancement efforts? Effects of financial risk and security level on evaluations of customer authentication", *International Journal of Human-Computer Studies*, ScienceDirect, vol. 70, s. 364–376, 2012, Accessed: 2022-02-08.

[80] O. N. Boateng, M. Asante ja I. K. Nti, "Implementation of Advanced Encryption Standard Algorithm with Key Length of 256 Bits for Preventing Data Loss in an Organization", *International Journal of Science and Engineering Applications*, Academia, vol. 6, s. 88–94, 2017, Accessed: 2022-02-08.

[81] G. Stoneburner, A. Goguen ja A. Feringa, *Risk Management Guide for Information Technology Systems*, Accessed: 2022-02-08, National Institute of Standards ja Technology, 2002.

[82] A. Josang, "The difficulty of standardizing smart card security evaluation", *Computer Standards & Interfaces*, ScienceDirect, vol. 17, s. 333–341, 1995, Accessed: 2022-02-08.

[83] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron ja K. Seamons, "A Usability Study of Five Two-Factor Authentication Methods", *Fifteenth Symposium on Usable Privacy and Security*, Brigham Young University, vol. 15, s. 357–370, 2019, Accessed: 2022-05-09.

[84] D. Goodin, *Microsoft says mandatory password changing is "ancient and obsolete"*, `https://arstechnica.com/information-technology/2019/06/microsoft-says-mandatory-password-changing-is-ancient-and-obsolete/`, Accessed: 2022-02-10, Ars Technica, 2019.

[85] Google Support, *Kadonneen Android-laitteen etsiminen, lukitseminen ja tyhjentäminen*, `https://support.google.com/accounts/answer/6160491?hl=fi`, Accessed: 2022-02-10.

[86] PassCamp, *Why choose password manager with two factor authentication?*, `https://www.passcamp.com/blog/why-choose-password-manager-with-two-factor-authentication/`, Accessed: 2022-02-24.

[87] Tietosuojavaltuutetun toimisto, *Rekisteröidyn suostumus*, `https://tietosuoja.fi/rekisteroidyn-suostumus`, Accessed: 2022-05-03.