Mikael Ruotsalainen

Ekku Sipilä

Itsehallittava identiteetti: määritelmä, komponentit sekä koetut hyödyt ja haasteet

Tietotekniikan ja tietojärjestelmätieteen pro gradu -tutkielma

24. huhtikuuta 2023

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijät: Mikael Ruotsalainen ja Ekku Sipilä

Yhteystiedot: mijojuru@student.jyu.fi ja eksasipi@student.jyu.fi

Ohjaajat: Antti-Jussi Lakanen ja Gabriella Laatikainen

Työn nimi: Itsehallittava identiteetti: määritelmä, komponentit sekä koetut hyödyt ja haasteet

Title in English: Self-sovereign identity: definition, components and perceived benefits and challenges

Työ: Pro gradu -tutkielma

Opintosuunta: Tietojärjestelmätiede ja tietotekniikka

Sivumäärä: 96+14

Tiivistelmä: Ihmisten käyttäessä yhä enemmän internetiä ja sen tarjoamia palveluita, korostuu myös digitaalisten identiteettien rooli ihmisten elämässä. Itsehallittava identiteetti on uusi lähestymistapa digitaaliseen identiteettiin, jossa käyttäjä on itse hallinnassa omista tiedoistaan ja niiden jakamisesta. Tämän tutkielman tavoitteena oli tutkia itsehallittavan identiteetin määritelmää ja sen tärkeimpiä komponentteja sekä selvittää sen käyttämiseen liittyviä potentiaalisia hyötyjä ja haasteita. Tutkimus koostui kahdesta osasta: systemaattisesta kirjallisuuskartoituksesta sekä kyselytutkimuksesta. Systemaattisella kirjallisuuskartoituksella pyrittiin selvittämään itsehallittavan identiteetin määritelmää ja sen tärkeimpiä komponentteja sekä kartoittamaan kirjallisuudessa esiintyviä itsehallittavan identiteetin hyötyjä ja haasteita. Tulokset osoittivat SSI:n määritelmien jaottuvan kolmeen eri tyyppiin: SSI paradigmana, SSI identiteetinhallintajärjestelmänä ja SSI digitaalisen identiteetin muotona. Tärkeimmiksi komponenteiksi osoittautuivat DID ja VC. Kyselytutkimuksen tavoitteena taas oli selvittää mahdollisten loppukäyttäjien näkemyksiä itsehallittavasta identiteetistä. Kyselyssä käytettiin Suomen uuden digitaalisen henkilöllisyystodistuksen hanketta havainnollistavana esimerkkinä sekä systemaattisen kirjallisuuskartoituksen tuloksia kysymysten pohjana. Kyselyyn vastasi 226 henkilöä. Saadun aineiston analysoinnissa hyödynnettiin sekä määrällisiä että laadullisia menetelmiä. Kyselyn tulokset osoittivat, ettei loppukäyttäjien

kokemuksissa ollut erityisen suuria eroja SSI:n hyötyihin liittyen. Tärkeimmäksi koettiin kuitenkin tietoturvan ja yksityisyyden kehittyminen sekä itsehallittavuus. Haasteisiin liittyen vastaajien kokemuksissa näkyi enemmän vaihtelua. Suurimmiksi haasteiksi koettiin uudet tietoturvatuhat, identiteettivarkaus sekä tunnusten palauttamiseen ja identiteettitietojen mahdolliseen väärinkäyttöön liittyvät haasteet.

Avainsanat: SSI, itsehallittava identiteetti, Suomen digitaalinen henkilöllisyystodistus, identiteetti, digitaalinen identiteetti, identiteetinhallintajärjestelmät

Abstract: As people increasingly use the internet and the services it provides, the role of digital identities in people's lives is also becoming more important. Self-sovereign identity is a new approach to digital identity, where users are in control of their own information and how they share it. Unlike previous identity management models, the user is put at the centre in the self-sovereign identity. The aim of this thesis was to explore the definition of self-sovereign identity and its main components, as well as the potential benefits and challenges associated with it. The study consisted of two parts: a systematic mapping and a survey. The systematic mapping aimed to identify the definition of self-sovereign identity and its main components, as well as to identify the benefits and challenges of self-sovereign identity in the literature. The results showed that definition of SSI falls into three different types: SSI as a paradigm, SSI as an identity management system and SSI as a form of digital identity. DID and VC emerged as the most important components. The survey, on the other hand, aimed to explore the perceptions of potential end-users on self-sovereign identity. The Finland's new digital ID project was used as an illustrative example and the results of a systematic mapping as a basis for the questions. 226 people responded to the survey. Both quantitative and qualitative methods were used to analyse the data. The results showed that there were no particularly large differences in end-users' perceptions of the importance of the benefits of different SSIs. However, the most important aspects were perceived to be the development of security and privacy, and self-sovereignty. There was more variation in the perception of challenges. New security threats, identity theft and challenges related to password recovery and possible misuse of identity data were perceived as the main challenges.

Keywords: SSI, self-sovereign identity, Finnish digital ID, identity, digital identity, IDMS

Kuviot

Kuvio 1. Keskitetty identiteetti 7
Kuvio 2. Federoitu identiteetti 8
Kuvio 3. DID-tunnisteen osat 16
Kuvio 4. DID:n komponentit ja niiden väliset vuorovaikutussuhteet 17
Kuvio 5. Väitteen, valtuustiedon ja valtuusesityksen komponentit 19
Kuvio 6. Luottamuksen kolmio 21
Kuvio 7. Digitaalisten agenttien vertaisverkkoyhteyden muodostus 27
Kuvio 8. Kirjallisuuskartoituksen prosessi 31
Kuvio 9. Hakuprosessin toteutus 37
Kuvio 10. Tutkimuskohteet ja niiden määrät 45
Kuvio 11. SSI:n määritelmän kategoriat 47
Kuvio 12. Kartoituksessa valittujen artikkeleiden yleisimmät viittaukset 50
Kuvio 13. SSI:n keskeisimmät komponentit 51
Kuvio 14. Vastaukset kysymykseen 8 64
Kuvio 15. Vastaukset kysymykseen 9 65
Kuvio 16. Vastaukset kysymykseen 11 67
Kuvio 17. Vastaukset kysymykseen 12 68

Taulukot

Taulukko 1. Allenin SSI:n ohjenuorat 12
Taulukko 2. Sovrinin kategorisointi SSI:n ohjenuorille 13
Taulukko 3. Potentiaaliset hyödyt 52
Taulukko 4. Potentiaaliset haasteet 55
Taulukko 5. Vastaajien ikä, koulutus ja pääasiallinen toimi määrittäin 60
Taulukko 6. Vastaajien työalat määrittäin 61
Taulukko 7. Vastaajien IT-taidot ja aihetuntemus 62
Taulukko 8. Vastaukset kysymykseen 8 63
Taulukko 9. Vastaukset kysymykseen 11 66
Taulukko 10. Rotatoitu faktorimatriisi 73

Sisällys

1 JOHDANTO 1
1.1 Motivaatio 1
1.2 Tutkimuskysymykset ja rakenne 2

2 ITSEHALLITTAVA IDENTITEETTI 4
2.1 Identiteetti ja digitaalinen identiteetti 4
2.1.1 Digitaalisen identiteetin mekanismit 5
2.1.2 Identiteetinhallintajärjestelmät 6
2.2 Itsehallittava identiteetti 10
2.3 Itsehallittavan identiteetin käytännön ratkaisut 14
2.4 Itsehallittavan identiteetin komponentit 15
2.4.1 Hajautettu tunniste (DID) 16
2.4.2 Todennettavat valtuustiedot 17
2.4.3 Luottamuksen kolmio 19
2.4.4 Verifioitavissa oleva tietorekisteri 20
2.4.5 Julkisen avaimen infrastruktuuri 21
2.4.6 Hajautettu tilikirjojen teknologia 22
2.4.7 Älysopimukset 23
2.4.8 Tietovarasto 24
2.4.9 Digitaalinen lompakko 25
2.4.10 Nollatietotodiste 27

3 TUTKIMUSMENETELMÄ 29
3.1 Motivaatio 29
3.2 Taustatieto 30
3.2.1 Systemaattinen kirjallisuuskartoitus 30
3.2.2 Kyselytutkimus 32
3.3 Systemaattinen kirjallisuuskartoitus 33
3.3.1 Tietokannat ja hakulausekkeet 34
3.3.2 Valintakriteerit 34
3.3.3 Aineiston hallinta 35
3.3.4 Pilotointi 36
3.3.5 Tutkimuksen toteutus 36
3.3.6 Kartoituksen validointi 37
3.3.7 Aineiston analysointi 38
3.4 Kyselytutkimus 39
3.4.1 Suomen digitaalinen henkilöllisyystodistus 39
3.4.2 Tutkimuksen toteutus 40
3.4.3 Tulosten analysointi 42
3.4.4 Kyselyn validiteetti 43

4 KIRJALLISUUSKARTOITUKSEN TULOKSET 44
4.1 Tutkimuskohde 44

4.2 SSI:n määritelmä ja keskeisimmät komponentit 46
4.3 Potentiaaliset hyödyt 51
4.4 Potentiaaliset haasteet 54

5 KYSELYTUTKIMUKSEN TULOKSET 59
5.1 Tausta- ja esitiedot 59
5.2 Koetut hyödyt 63
5.3 Koetut haasteet 65
5.4 Avointen kysymysten vastaukset 68
5.5 Eksploratiivinen faktorianalyysi 72

6 JOHTOPÄÄTÖKSET JA POHDINTA 74
6.1 Tutkimustulokset ja niiden teoreettiset kontribuutiot 74
6.1.1 Systemaattinen kirjallisuuskartoitus 74
6.1.2 Kyselytutkimus 76
6.2 Tulosten merkitys käytäntöön 78
6.3 Rajoitteet 79
6.4 Jatkotutkimus 80

7 YHTEENVETO 82

LÄHTEET 84

LIITTEET 91
A Kyselylomake 92
B Kirjallisuuskartoitus: hakulausekkeen kehitys 99
C Kirjallisuuskartoituksen tulokset: potentiaaliset hyödyt 101
D Kirjallisuuskartoituksen tulokset: potentiaaliset haasteet 103

1 Johdanto

Tämän pro gradu -tutkielman tutkimuskohteena on itsehallittava identiteetti (engl. self-sovereign identity), lyhemmin SSI. Tutkielman tavoitteena on tutkia SSI:tä käsitteenä sekä selvittää siihen liittyviä hyötyjä ja haasteita. Tässä luvussa käsitellään ensin kirjoitelman motiiveja, jonka jälkeen käydään läpi tutkimuskysymykset ja tutkielman rakenne.

1.1 Motivaatio

Ihmiset viettävät yhä enemmän aikaa internetissä, maailma digitalisoituu kovaa vauhtia ja tietotekniikka integroituu yhä useampaan osa-alueeseen ihmisten elämässä. Tämän takia digitaalisten identiteettien käyttö ja tärkeys on lisääntynyt huomattavasti. Digitalisoitumisen myötä myös informaation keräys on tehostunut ja sen määrä on lisääntynyt valtavasti. Allenin (2016) mukaan hallitukset ja yritykset jakavat ja käyttävät ennennäkemättömän paljon tätä tietoa. Tämä informaatio kattaa ihmisten katselutottumukset ja ostokset sekä sen, missä ihmiset oleskelevat päivisin, nukkuvat öisin ja kenen kanssa he ovat tekemisissä (Allen 2016). Samalla, datan siiloutuminen eli keskittyminen yhteen paikkaan voi heikentää tietoturvaa sekä lisää tietovuotoja tahattoman jakamisen vuoksi (Tobin ja Reed 2016).

Digitaalisten identiteettien ja niiden hallintajärjestelmien malleja on kehitetty paljon. Itsehallittavaa identiteettiä voidaan pitää viimeisimpänä kehitysaskeleena näistä malleista. Itsehallittavassa identiteetissä käyttäjällä on täysi kontrolli ja valta omaan identiteettiinsä ja siihen liittyvään informaatioon (Mühle ym. 2018; Allen 2016; Wang ja De Filippi 2020). Vanhempia identiteetinhallintajärjestelmiä käytetään kuitenkin vielä lähes kaikissa järjestelmissä ja nettisivuilla. Näistä yleisimpiä ovat keskitetty identiteetti ja federoitu identiteetti, joissa hallinta ja data ovat siiloutuneet sekä ne on keskitetty yhteen paikkaan (Naik ja Jenkins 2020a). Lisäksi näissä malleissa käyttäjillä on vain vähän valtaa omista tiedoistaan (Allen 2016).

SSI korjaisi paljon näitä vanhempiin ja käytössä oleviin malleihin liittyviä ongelmia. Jotta SSI voitaisiin ottaa käyttöön laajamittaisesti, on sitä kuitenkin tutkittava enemmän (Wang ja De Filippi 2020). On myös paljon asioita, joita ei vielä ole standardoitu, tai joista ei ole

päästy yhteisymmärrykseen tiedeyhteisöissä (Naik ja Jenkins 2020a; Mühle ym. 2018). Tästä syystä tutkielman aihe on hyvin ajankohtainen ja tutkimus tarpeellinen.

Suomen Digi- ja väestövirasto (2023) on myös tutkielman toteutuksen aikaan kehittämässä hanketta uudesta digitaalisesta henkilöllisyystodistuksesta, jonka toiminta pohjautuu itsehallittavaan identiteettiin. Se on uusi käytännön sovellutus identiteetinhallintajärjestelmästä, joka pohjautuu itsehallittavaan identiteettiin. Tutkielman kyselytutkimus pohjautuu ja tarkastelee vastaajien näkemyksiä tästä hankkeesta.

1.2 Tutkimuskysymykset ja rakenne

Tutkielman tavoitteena on tutkia itsehallittavaan identiteettiin liittyviä potentiaalisia hyötyjä ja haasteita sekä selvittää sen määritelmä ja tärkeimmät komponentit. Tutkielman tutkimuskysymykset ovat siis seuraavat:

1. Mikä on itsehallittavan identiteetin määritelmä ja mitkä ovat sen tärkeimmät komponentit?
2. Mitä potentiaalisia hyötyjä ja haasteita itsehallittavaan identiteettiin liittyy käyttäjän näkökulmasta?
3. Mitkä ovat olennaisimmat itsehallittavan identiteetin hyödyt ja haasteet Suomen digitaalisen henkilöllisyystodistuksen kontekstissa loppukäyttäjän näkökulmasta?

Tutkimus koostuu kahdesta tutkimuksesta: systemaattisesta kirjallisuuskartoituksesta sekä kyselytutkimuksesta. Systemaattisen kirjallisuuskartoituksen avulla etsitään vastausta tutkimuskysymyksiin 1 ja 2. Kyselytutkimuksen avulla etsitään vastausta tutkimuskysymykseen 3.

Tutkielmaan kuuluu seitsemän eri lukua. Luku 1 on tämä luku eli johdanto. Luvussa 2 käsitellään tutkimukseen liittyvää teoriaa ja keskeistä termistöä. Luvussa 3 käydään läpi tutkielman tutkimusmenetelmät ja -prosessit kumpaankin tutkimukseen liittyen. Tämän lisäksi luvussa käydään läpi tutkimuksiin liittyvää taustatietoa sekä esitellään Suomen uuden digitaalisen henkilöllisyystodistuksen hanke. Luvussa 4 esitellään kirjallisuuskartoituksen tulokset, ja luku 5 taas käsittelee kyselytutkimuksen tuloksia. Seuraavaksi on luku 6, eli

pohdinta-luku, jossa tarkastellaan kummankin tutkimuksen tuloksia kokonaisuutena, tutkimusten rajoitteita sekä esitellään jatkotutkimusehdotuksia. Viimeisenä on luku 7, joka on yhteenveto koko tutkielmasta.

2 Itsehallittava identiteetti

Tässä luvussa käsitellään tutkimukseen liittyvää taustaa ja teoriaa sekä esitellään tutkimuksen keskeistä termistöä. Aluksi keskustellaan digitaalisesta identiteetistä ja sen mekanismeista. Sitten käsitellään identiteetinhallintajärjestelmiä keskittyen varsinkin itsehallittavaan identiteettiin. Tämän jälkeen esitellään itsehallittavan identiteetin olennaisimmat komponentit. Teorian käsittelyssä hyödynnetään suoritettua systemaattista kirjallisuuskartoitusta, sen tuloksia sekä tuloksista esiin nousseita hyödyllisiä artikkeleita.

2.1 Identiteetti ja digitaalinen identiteetti

Identiteetti voidaan määritellä monelta eri kantilta. Wang ja De Filippi (2020, s. 2) esittävät identiteetille määritelmiä psykologisen, sosiologisen sekä juridisen näkökulman kautta. Tärkeimpänä he esittävät kuitenkin identiteetin "kuvaamaan kaikkia niitä henkilön ominaisuuksia, jotka määrittelevät henkilön ainutlaatuisesti koko eliniän ajan ja takaavat samankaltaisuuden ja jatkuvuuden erilaisista näkökohdista ja olosuhteista huolimatta." Identiteetti voidaan selittää myös "eksklusiivisena näkemyksenä elämästä, sosiaaliseen ryhmään integroitumisena tai jatkuvuutena, joka on sidottu johonkin kehoon ja on, ainakin jossain määrin, yhteiskunnan muovaama" (Pfitzmann ja Hansen 2010, s. 29). Matemaattisen ja tietoteknisen näkökulman kautta Camp (2004) esittää identiteetin olevan johonkin entiteettiin liittyvien ikuisesti säilyvien tai pitkäkestoisten ominaisuuksien kokonaisuus. Samaan tapaan Modinis (2005) esittää, että identiteetti on dynaaminen kokoelma kaikista tietyn entiteetin attribuuteista. Lisäksi yhdellä entiteetillä on vain yksi identiteetti. Entiteetti voi olla esimerkiksi henkilö, mutta myös paljon muuta. Identiteetti viittaa siis kaikkeen siihen, mikä luonnehtii kohdetta, kuten esimerkiksi henkilöä. (López 2020)

Modinis (2005) mukaan *digitaalinen identiteetti* on sähköisessä muodossa oleva osittainen identiteetti. Osittainen identiteetti taas on yhden tai useamman ominaisuuden tietty osajoukko, joka ei välttämättä määrittele henkilöä ainutlaatuisesti. Lähes jokaisella henkilöllä on yleensä monia digitaalisia identiteettejä, jotka voivat olla yksilöiviä tai ei-yksilöiviä. Tässä mielessä digitaalinen identiteetti on identiteetin osajoukko, ja sitä voidaan pitää osoi-

tuksena henkilön läsnäolosta sähköisissä järjestelmissä (Modinis 2005). Myös Mühle ym. (2018) mukaan digitaalinen identiteetti on yksinkertaisesti kuvattuna keino, jolla ihmiset voivat sähköisesti todistaa olevansa sitä, mitä he sanovat olevansa, ja erottaa eri tahot toisistaan. Pfitzmann ja Hansen (2010) mukaan digitaalinen identiteetti viittaa siihen, että yksittäiselle henkilölle osoitetaan attribuuttiarvoja, jotka ovat välittömästi tarkasteltavissa ja käytettävissä teknologisten välineiden avulla. Attribuutteja voi olla esimerkiksi nimi ja käyttäjätunnus. Digitaalinen identiteetti on siis rajallinen joukko ominaisuuksia, joiden avulla henkilö voidaan tunnistaa ja todentaa muille sähköisesti (López 2020).

2.1.1 Digitaalisen identiteetin mekanismit

Digitaalisen identiteetin keskeisimmät mekanismit ovat identifiointi, autentikointi ja auktorisointi. Identifiointi (engl. Identification) on toimijan väite sen identiteetistä, kun taas autentikointi (engl. Authentication) on tämän identiteetin tunnistamista tai todentamista. Auktorisointi (engl. Authorization) on mekanismi, jolla tarkistetaan toimijan valtuudet käyttää palvelua. Campin (2004) mukaan identifiointi on ominaisuuksia omaavan henkilökohtaisen tunnisteen yhdistäminen yksilöön. Esimerkkeinä voidaan mainita fyysisen henkilön ja väitetyn nimen oikeellisuuden todentaminen, yrityksen ja rahoitustietojen välisen yhteyden määrittäminen tai potilaan yhdistäminen fyysisten ominaisuuksien tietueeseen. Identifiointi edellyttää toimiakseen yksilöivän tunnisteen, kuten vaikkapa käyttäjätunnuksen tai sähköpostiosoitteen (Camp 2004). Jos esimerkiksi identifiointi viittaa käyttäjätunnukseen, viittaa autentikointi käyttäjätunnuksen ja salasanan yhdistelmään (Ferdous, Chowdhury ja Alassafi 2019). Jonkin salaisen tunnisteen, kuten salasanan, yhdistäminen käyttäjätunnukseen varmistaa sen, että kirjautuja on identiteetin todellinen haltija. Identifioinnin ja identiteetin autentikoinnin erot selittyvät myös hyvin Campin (2004) esimerkissä: “Olet John Doe” viittaa identifiointiin, kun taas “asiakirjasi osoittavat, että olet John Doe” viittaa identiteetin autentikointiin. Autentikointiin on monia eri menetelmiä. Dib ja Toumi (2020) esittävät seuraavat menetelmät:

- Jotain, minkä tiedät, kuten PIN-koodi tai salasana.
- Jotain, joka sinulla on, kuten henkilökortti, pankkikortti, älykortti, turvamerkki, matkapuhelin tai henkilöllisyystodistus.

- Jotain, mitä olet, kuten sormenjäljet, kasvot, iirikset ja ääni.
- Jotain, mitä teet, kuten motoriset taidot, eleet ja näppäinpainallukset tai sovellukset.

Kun identifiointi- ja autentikointiprosessi on suoritettu onnistuneesti, siirrytään auktorisointiin. Auktorisoinnissa kohteelle myönnetään jokin valtuutus sen todistaman henkilöllisyyden perusteella. Tiettyjä toimia voidaan siis sallitaan kohteen ominaisuuksien perusteella. (Dib ja Toumi 2020) Esimerkkejä tästä ovat henkilön oikeus esittää luottovaatimuksia, hälytysajoneuvon oikeus ajaa punaisen valon läpi tai säteilyä kestävän laitteen sertifiointi rakenteilla olevaan satelliittiin kiinnitettäväksi (Camp 2004).

2.1.2 Identiteetinhallintajärjestelmät

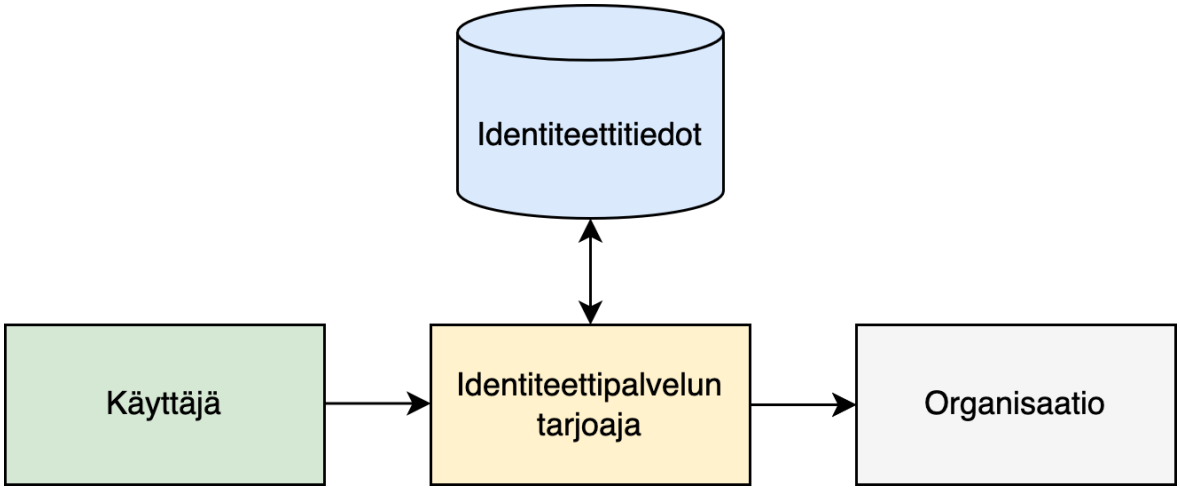
Identiteetinhallintajärjestelmät voidaan jakaa neljään eri kategoriaan: keskitetty identiteetti, federoitu identiteetti, käyttäjäkeskeinen identiteetti ja itsehallittava identiteetti (Shuaib, Hassan, Usman, Alam, Bhatia, Agarwal ym. 2022; Allen 2016; Ferdous, Chowdhury ja Alassafi 2019). Tässä luvussa esitellään ja vertaillaan näistä kolmea ensimmäistä. Itsehallittava identiteetti esitellään omassa luvussaan 2.2.

Keskitetty identiteetti (engl. Centralized Identity) on perinteisin identiteetinhallintajärjestelmä, ja nimensä mukaisesti siinä tietojen hallinta on keskitetty yhdelle osapuolelle. Yksilö käyttää identiteettijärjestelmää hallinnoivan tai omistavan organisaation palveluja. Tämä organisaatio kerää, säilyttää ja käyttää yksilön identiteettiä ja siihen liittyvää dataa ja henkilökohtaisesti tunnistettavia tietoja yksinoikeudella. (Dib ja Toumi 2020) Yksi esimerkki keskitystä identiteetistä on seuraava: Kun henkilö käyttää jonkin pankin palveluita, hän luo tunnukset pankkiin. Silloin tämä pankki kerää, säilyttää ja käyttää kaikkea sitä dataa, mitä syntyy, kun henkilö asioi käyttäen tämän pankin tunnuksia. Organisaation ja käyttäjän välinen luottamussuhde perustuu jaettuun salaisuuteen, joka useimmissa tapauksissa on yleensä käyttäjätunnus ja salasana. Käyttäjä tarvitsee erilliset tunnistetiedot jokaista organisaatiota tai järjestelmää varten, joista hän haluaa saada palvelua (Naik ja Jenkins 2020a). Käyttäjän täytyy myös muistaa kaikki tunnistetietonsa. Tämä on työlästä ja epäkäytännöllistä. Allenin (2016) mukaan keskitetty identiteetti antaa vallan käyttäjien sijaan keskitetyille yksiköille, sillä keskitetyillä yksiköillä on mahdollisuus käyttää käyttäjän dataa lain puitteissa miten

he haluavat, ilman että käyttäjällä on mahdollista vaikuttaa asiaan. Keskitetty identiteetti on mallinnettu kuviossa 1.

Kuvio 1: Keskitetty identiteetti (mukailtu Naik ja Jenkins 2020a)

Federoitu identiteetti (engl. Federated Identity) on tulosta kahden tai useamman keskitetyn järjestelmän yhteisen luottamuksen luomisesta (Dib ja Toumi 2020). Käytännössä tämä tarkoittaa, että keskitetyt järjestelmät ottavat käyttöön yhteisen, mahdollisesti kolmannen osapuolen tarjoaman, identiteettipalveluntarjoajan, joka hoitaa identiteetinhallinnan täysin heidän puolestaan. Naik ja Jenkins (2020a) esittävät federoidun identiteetin ratkaisevan kaksi identiteetinhallinnan ongelmaa: Identiteettien hallinnoimisen taakka poistuu organisaatioilta ja useiden tunnistetietojen hallinnoimisen taakka poistuu käyttäjiltä. Tämä malli on hyvin suosittu ympäristöissä, joissa identiteettidataa jaetaan vain luotettujen tahojen välillä, kuten valtioiden ja koulutusinstituutioiden palveluissa (Naik ja Jenkins 2020a). Suomen vahva tunnistautuminen (Suomi.fi -palvelu) on yksi esimerkki tästä mallista. Federoitu identiteetti jakaa kuitenkin keskitetyn mallin saman ongelman siitä, että identiteettipalveluntarjoajalla on hallussaan käyttäjän identiteettiin liittyviä henkilökohtaisesti tunnistettavia tietoja, eikä käyttäjällä ole niin paljon valtaa näiden omien tietojensa hallintaan (Naik ja Jenkins 2020a). Kuvio 2 mallintaa federoitua identiteettiä.



Kuvio 2: Federoitu identiteetti (mukailtu Naik ja Jenkins 2020a)

Federoitu identiteetti mahdollistaa myös kertakirjautumisen (engl. Single-Sign On, jatkossa SSO) ja sosiaalisen kirjautumisen (engl. Social login) -palvelut, jotka poistavat käyttäjiltä taakan hallita ja muistaa useita identiteettiin liittyviä tunnistetietoja useissa järjestelmissä. (Allen 2016; Naik ja Jenkins 2020a). SSO:lla tarkoitetaan mallia, jossa käyttäjä voi kirjautua yksillä tunnuksilla useampiin saman palveluntarjoajan järjestelmiin. Yksi esimerkki tästä on Google-tunnuksilla kirjautuminen Googlen eri palveluihin. Käyttäjä pystyy kirjautumaan samoilla tunnuksilla esimerkiksi Google Driveen sekä Google Docsiin. Sosiaalinen kirjautuminen taas viittaa siihen, että jonkin identiteettipalvelutarjoajan tunnuksilla kirjaudutaan toisen palveluntarjoajan järjestelmiin. Kun Google-tunnuksilla kirjaudutaankin johonkin muuhun kuin Googlen palveluun, kuten Ali Baba -verkkokauppaan, puhutaan sosiaalisesta kirjautumisesta. Tällöin Ali Baban ei tarvitse itse toteuttaa ja tarjota identiteetinhallintaa, vaan se ulkoistetaan Googlelle.

Käyttäjäkeskeinen identiteetti on hyvin samankaltainen kuin federoitu identiteetti, mutta siinä käyttäjällä on hieman enemmän valtaa. Kuten federoidussa mallissa, tässä mallissa useat palveluntarjoajat voivat jakaa yhden identiteettipalveluntarjoajan. Aina kun käyttäjä yrittää käyttää palveluntarjoajan palvelua, hänet ohjataan identiteettipalveluntarjoajalle, jossa hän todentaa itsensä. Tämän jälkeen identiteettipalveluntarjoaja luovuttaa käyttäjän identiteettitiedot profiilin avulla palveluntarjoajalle. (Ferdous, Chowdhury ja Alassafi 2019) Käyttäjä hallitsee itse tunnistetietojaan ja määrittelee, miten hän jakaa attribuuttejaan pal-

veluntarjoajan kanssa palvelun käyttämiseksi (P. Bai ym. 2022). Esimerkiksi kirjautuessa Facebook-tunnuksilla toiseen palveluun, tulee ensin ilmoitus, että kyseinen palvelu haluaa Facebookilta käyttäjän sähköpostin, nimen ja kuvan, joka käyttäjän pitää hyväksyä ennen tunnistautumisen tapahtumista. Palveluntarjoaja saa siis vain sen verran tietoa käyttäjästä, mitä käyttäjä haluaa sille antaa. Suurin osa tunnetuimmista identiteettipalveluntarjoajista, kuten Google ja Facebook, toteuttavat käyttäjäkeskeistä mallia (Ferdous, Chowdhury ja Alassafi 2019).

Käyttäjäkeskeisen identiteetin määritelmässä on edelleen epäselkeyksiä. Monesti käyttäjäkeskeinen identiteetti saatetaan jopa jättää määrittelemättä, vaikka federoidun ja keskitetyn identiteetin määritelmiä on käsitelty (esimerkiksi Dib ja Toumi 2020; Naik ja Jenkins 2020a). Myös käytännön esimerkit näistä malleista vaihtelevat. Ferdous, Chowdhury ja Alassafi (2019) määrittelevät nykyiset tunnetuimmat identiteettipalveluntarjoajat, kuten Google ja Facebookin, käyttäjäkeskeisiksi identiteeteiksi. Tämä johtuu siitä, että esimerkiksi kirjautuessa Facebook-tunnuksilla toiseen palveluun, tulee ensin ilmoitus palvelun pyytämistä tiedoista, joka käyttäjän pitää hyväksyä ennen tunnistautumisen tapahtumista. P. Bai ym. (2022) sekä Dib ja Toumi (2020) kuitenkin sanovat näiden olevan federoituja identiteettejä. P. Bai ym. (2022) taas määrittelevät käyttäjäkeskeisen identiteetin olevan hajautettu malli ja sanovat joidenkin hajautettujen identiteettipalveluntarjoajien, kuten uPortin, Shocardin ja BitID:n olevan käyttäjäkeskeiseen malliin pohjautuvia. Selvää yhteisymmärrystä mallin määritelmään ei siis ole.

Allenin (2016) mukaan käyttäjäkeskeisellä mallilla pyritään siihen tilanteeseen, että käyttäjä asetetaan identiteettiprosessin keskelle sekä sitä, että käyttäjä saa hallita omaa identiteettiään paremmin, ja että luottamus on hajautettu. Käyttäjäkeskeisen mallin avulla yritetään myös luoda parempaa käyttäjäkokemusta. Käyttäjäkeskeiset identiteetit eivät kuitenkaan ole vielä tulleet laajemmin käyttöön, joten keskitetyt tahot säilyivät yhä identiteettiprosessissa. (Allen 2016)

2.2 Itsehallittava identiteetti

Itsehallittava identiteetti (engl. Self-sovereign Identity, jatkossa lyhyesti SSI) nähdään uusimpana digitaalisena identiteetinhallintajärjestelmänä (Mühle ym. 2018). Itsehallittavasta identiteetistä puhutaan myös paradigmana tai konseptina (Ferdous, Chowdhury ja Alassafi 2019; Čučko ym. 2022; Wang ja De Filippi 2020) ja joissain vain uusimpana digitaalisen identiteetin muotona (Tobin ja Reed 2016; Wang ja De Filippi 2020).

Se on käsite, jota ei ole vielä kauaa olemassa, eikä sen käytännön toteutus ole vielä kauaa ollut mahdollista. Koska käsite on uusi, ei sen määritelmäkään ole vielä tieteellisesti yhtenäinen tai vakiintunut (Mühle ym. 2018; Ferdous, Chowdhury ja Alassafi 2019; Wang ja De Filippi 2020). On kuitenkin tiettyjä suosittuja teoksia, joihin viitataan usein SSI:n määrittelyssä. Näitä artikkeleita koottiin yhteen systemaattisen kirjallisuuskartoituksen aikana.

Vaikka itsehallittavasta identiteetistä ei olekaan vielä yhtenäistä määritelmää, on yhtäläisyyksiä määritelmissä kuitenkin monia. Lähes kaikissa artikkeleissa esitetään itsehallittavassa identiteetissä käyttäjä olevan täydessä kontrollissa omasta identiteetistään (Mühle ym. 2018; Allen 2016; Wang ja De Filippi 2020). Käyttäjän täyteen kontrolliin liittyy myös se, ettei kolmatta osapuolta tarvita lainkaan datan käsittelyyn, tallentamiseen tai päivittämiseen, eikä mihinkään muuhunkaan (Mühle ym. 2018; Dib ja Toumi 2020; Daniela Pöhn, Michael Grabatin ja Wolfgang Hommel 2021). Useimmiten itsehallittavan identiteetin toteuttamiseksi hyödynnetään lohkoketjuteknologiaa. Tämän teknologian synty mahdollisti ensimmäistä kertaa itsehallittavan identiteetin käytännön toteutuksen. Lohkoketjuteknologia ei kuitenkaan ole ainut tapa toteuttaa itsehallittava identiteetti (Čučko ym. 2022; Nokhbeh Zaeem ym. 2021; Stokkink ja Pouwelse 2018; Schardong ja Custódio 2022), vaikka se onkin tällä hetkellä toimivin vaihtoehto. Schardong ja Custódio (2022) jopa väittävät, että täyden itsehallittavuuden saavuttamiseksi käyttäjän ei pitäisi joutua luottamaan kehenkään, ei siis edes lohkoketjuteknologiaan.

Christopher Allenin blogikirjoitus itsehallittavasta identiteetistä on viitatuin kirjoitus sen määritelmään liittyen. Allen (2016) määrittelee itsehallittavan identiteetin seuraavalla tavalla:

> ... käyttäjän on oltava keskeisessä asemassa identiteetin hallinnoinnissa. Tä-

> mä edellyttää käyttäjän identiteetin yhteensopivuutta useissa eri sijainneissa, käyttäjän suostumuksen tarvetta kaikille tapahtumille sekä käyttäjän todellista lupaa hallita digitaalista identiteettiään, mikä luo käyttäjälle autonomian. Tämän saavuttamiseksi itsehallittavan identiteetin on oltava siirrettävissä; sitä ei voi lukita yhteen sijaintiin tai paikkaan. Itsehallittavan identiteetin on myös annettava tavallisille käyttäjille mahdollisuus esittää väitteitä, jotka voivat sisältää henkilökohtaisia tunnistetietoja tai tietoja henkilökohtaisista kyvyistä tai ryhmän jäsenyydestä. Se voi jopa sisältää tietoja käyttäjästä, jotka muut henkilöt tai ryhmät ovat esittäneet.

Allen (2016) esittää myös kymmenen ohjenuoraa, joiden tulisi toteutua itsehallittavaa identiteettiä toteuttaessa:

Ohjenuora	Kuvaus
1. Olemassaolo (existance)	Käyttäjillä on oltava itsenäinen olemassaolo, ne eivät voi olla olemassa vain täysin digitaalisena. Identiteetistä tuodaan julki vain rajattuja osia.
2. Kontrolli (control)	Käyttäjät hallitsevat itse identiteettiään. Heillä tulee olla oikeus ja mahdollisuus piilottaa, julkaista ja päivittää tietojaan.
4. Läpinäkyvyys (transparency)	Järjestelmien ja algoritmien on oltava avoimia niiden toiminnan, hallinnan ja esimerkiksi päivittämisen suhteen.
5. Pysyvyys (persistence)	Identiteettien on oltava pitkäikäisiä, mielellään niiden tulisi pystyä säilymään ikuisesti. Tämä ei saa kuitenkaan mennä päällekkäin käyttäjän oikeuteen pystyä poistamaan tietojaan.
6. Siirrettävyys (portability)	Identiteettiä koskevien tietojen ja palvelujen on oltava siirrettävissä.
7. Yhteensopivuus (interoperability)	Tunnusten olisi oltava mahdollisimman laajasti käytettävissä saavuttaakseen parhaan hyödyn.
8. Suostumus (consent)	Käyttäjien on annettava hyväksyntä heidän henkilöllisyytensä käyttöön sekä heidän tietojensa jakamiseen.
9. Minimointi (minimalization)	Tietoa tulee saada jakaa ehdoton tarvittava minimimäärä, mitä tarvitaan, jotta tehtävä saadaan suoritettua.
10. Suojaus (protection)	Käyttäjien oikeuksia on suojeltava ja käyttäjä on laitettava etusijalle turvallisuuden hallinnassa.

Taulukko 1: Allenin kymmenen ohjenuoraa itsehallittavalle identiteetille (mukailtu Allen 2016)

Toinen laajasti viitattu lähde on Sovrin -säätiö, joka on itsehallittavan identiteetin käyttöön perustuva verkosto. Sovrin määrittelee itsehallittavan identiteetin valkoisessa kirjassaan seuraavalla tavalla: (Tobin ja Reed 2016)

> Henkilö (tai organisaatio), johon identiteetti liittyy, omistaa, valvoo ja hallinnoi identiteettiään täysin. Tässä mielessä yksilö on oma identiteetin tarjoajansa - mikään ulkopuolinen taho ei voi väittää "tarjoavansa" identiteettiä heille, koska identiteetti on luonnostaan heidän. ... Voit paljastaa osan siitä tai sen kokonaan, osan ajasta tai kaiken aikaa. Voit antaa suostumuksesi tietojen jakamiseen muiden kanssa ja suorittaa sen helposti. Se on pysyvää eikä ole riippuvainen mistään yksittäisestä kolmannesta osapuolesta. Tunnistustapahtumissa sinusta esitetyt väitteet voivat olla joko itse esitettyjä tai kolmannen osapuolen esittämiä, joiden todenperäisyyden voi varmistaa riippumaton osapuoli.

Samassa kirjassa Sovrin myös kategorisoi Allenin yllä mainitut kymmenen ohjenuoraa kolmeen kategoriaan, jotka ovat turvallisuus, hallittavuus ja siirrettävyys:

Kategoria	Ohjenuora
Turvallisuus	Suojaus
	Pysyvyys
	Minimointi
Hallittavuus	Olemassaolo
	Pysyvyys
	Kontrolli
	Suostumus
Siirrettävyys	Yhteensopivuus
	Läpinäkyvyys
	Pääsy

Taulukko 2: Sovrinin kategorisointi Allenin esittämille ohjenuorille (mukailtu Tobin ja Reed 2016)

Ferdous, Chowdhury ja Alassafi (2019) esittävät artikkelissaan laajennetun version Allenin itsehallittavan identiteetin taksonomiasta. He lisäsivät määritelmään perusteellisuuden (engl. foundational), joustavuuden (engl. flexibility) ja kestävyyden (engl. sustainability). Lisäksi he esittivät lait itsehallittavalle identiteetille pohjautuen aiempaan taksonomiaan. Čučko ym. (2022) esittävät artikkelissaan 18 eri itsehallittavan identiteetin ominaisuutta, jotka he kokosivat olemassa olevasta kirjallisuudesta. Naik ja Jenkins (2020a) esittävät myös 20 ohjenuoraa itsehallittavan identiteetin hallinnointiin. Nämä ohjenuorat perustuvat Allenin kymmeneen ohjenuoraan, sekä James Cameronin identiteetin lakeihin (Cameron 2005).

2.3 Itsehallittavan identiteetin käytännön ratkaisut

Koska itsehallittava identiteetti on käsitteenä ja ilmiönä uusi, ei sitä ole vielä otettu laajalti käyttöön käytännön tasolla. Käytännön ratkaisuja mahdollistavia työkaluja on kuitenkin jo olemassa ja niiden määrä on kasvussa (Liu ym. 2020). Shuaib, Hassan, Usman, Alam, Bhatia, Agarwal ym. (2022) mukaan suosituimpia esimerkkejä käytännön ratkaisuista ovat Sovrin (Tobin ja Reed 2016), uPort (Lundkvist ym. 2016), Blockstack (Ali ym. 2016), Selfkey (Foundation 2017) ja ShoCard (Ebrahimi 2019). Näistä ratkaisuista tutkimuksissa puhutaan eniten Sovrinista sekä uPortista (Naik ja Jenkins 2020c; Liu ym. 2020; Schardong ja Custódio 2022). Tästä syystä tässä kappaleessa esitellään käytännön ratkaisuista Sovrin ja uPort. Näiden lisäksi luvussa 3.3.1 keskustellaan Suomen uudesta digitaalisesta henkilöllisyystodistuksesta, joka on yksi esimerkki itsehallittavaan identiteettiin pohjautuvan identiteetinhallintajärjestelmän käyttöönotosta.

Sovrin on avoimen lähdekoodin ratkaisu itsehallittavalle identiteetille. Siinä identiteetti ei ole riippuvainen mistään keskitetystä tahosta, eikä sitä ole mahdollista poistaa (Liu ym. 2020). Käyttäjän henkilökohtaista dataa kerätään ja säilytetään käyttäjän omalla laitteella, kuten puhelimella, tai käyttäjän hyväksymillä agenteilla, jotka eivät ole kolmannen osapuolen palveluntarjoajia (Shuaib, Hassan, Usman, Alam, Bhatia, Agarwal ym. 2022). Sovrin pohjaa toimintansa Hyperledger Indy -lohkoketjuun, joka on suljettu (engl. permissioned) lohkoketju (Naik ja Jenkins 2020c). Sovrinin tapauksessa lohkoketjun lukeminen on avointa kaikille, mutta kirjoittaminen ja ketjun validointi rajattua. Itse identiteetit tallen-

tuvat lohkoketjuun, jossa kaikkien on mahdollista käyttää ja todentaa niitä (Shuaib, Hassan, Usman, Alam, Bhatia, Agarwal ym. 2022). Naik ja Jenkins (2020c, s. 4) tiivistävät Sovrinin toiminnan seuraavalla tavalla: “Sovrinin ratkaisun avulla käyttäjät voivat turvallisesti julkaista identiteettinsä, mukaan lukien valtakirjojensa siirtämisen, tapahtumien allekirjoittamisen sekä avaintensa ja tietojensa hallinnan. Sovrin-identiteetti voidaan luoda käyttäjille, organisaatioille tai muille resursseille. Sovrin antaa käyttäjille mahdollisuuden luoda eri identiteettejä, joilla kaikilla on omat yksityiset ja julkiset avaimet eri yhteyksissä luottamuksen säilyttämiseksi. Käyttäjä määrittää itse, minkä tyyppisiä attribuutteja hänen identiteettiinsä liitetään. Sovrin käyttää nimettömiä tunnistetietoja, jotka perustuvat nollatietotodiste -kryptografiamenetelmään, jotta käyttäjän identiteetit pysyvät nimettöminä.”

Toinen esimerkki SSI:n käytännön ratkaisuista on nimeltään uPort. Uportin valkoisen kirjan mukaan uPort on Ethereum-lohkoketjuun rakennettu turvallinen ja helppokäyttöinen järjestelmä itsehallittaville identiteeteille. Uport-teknologia koostuu kolmesta pääkomponentista: älysopimuksista, kehittäjäkirjastoista (engl. developer library) ja mobiilisovelluksesta. Mobiilisovellukseen tallentuvat käyttäjän avaimet. Älysopimukset muodostavat identiteetin ytimen sisältäen toiminnan, jonka avulla käyttäjä voi palauttaa identiteettinsä, mikäli hänen mobiililaitteensa katoaa. Kehittäjäkirjastojen avulla kolmannen osapuolen sovelluskehittäjät voivat integroida omat sovelluksensa yhteensopiviksi uPortin kanssa. (Lundkvist ym. 2016) Uportin suurin ero Sovriniin toiminnassa on, että Sovrin käyttää suljettua lohkoketjuteknologiaa hyödykseen, kun taas uPort avointa (engl. permissionless) lohkoketjua. Uportin tapauksessa kuka vain voi validoida ja kirjoittaa lohkoketjuun, kun taas Sovrinin tapauksessa tämä on rajattua. Lisäksi Sovrin käyttää yksityisyyden suojaukseen nollatietotodisteita, kun taas uPort ei (Naik ja Jenkins 2020c). Tämän sijaan uPort käyttää käyttäjän yksityisyyden suojaamiseksi esimerkiksi valikoivaa julkistamista (engl. selective disclosure) (Lundkvist ym. 2016). Lisää avoimista ja suljetuista lohkoketjuista kerrotaan luvussa 2.4.6.

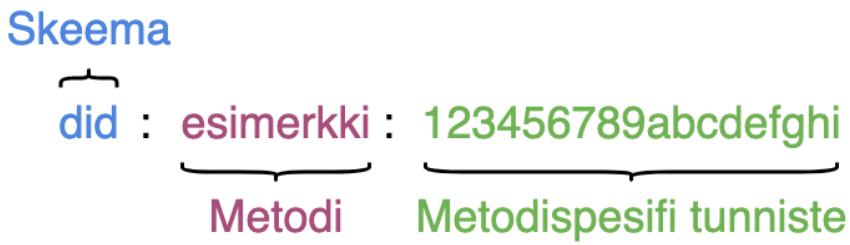
2.4 Itsehallittavan identiteetin komponentit

Tässä luvussa esitellään kymmenen SSI:n keskeisintä komponenttia. Nämä komponentit löytyivät kirjallisuuskartoituksen tuloksena. Komponentit avataan vain lyhyesti, jotta tutki-

muksen tuloksia on helpompi tulkita. Lisäksi komponentteja pyritään käsittelemään itsehallittavan identiteetin näkökulmasta, eli niillä saattaa olla kattavampiakin määritelmiä, jotka voidaan mahdollisesti sivuuttaa tässä luvussa.

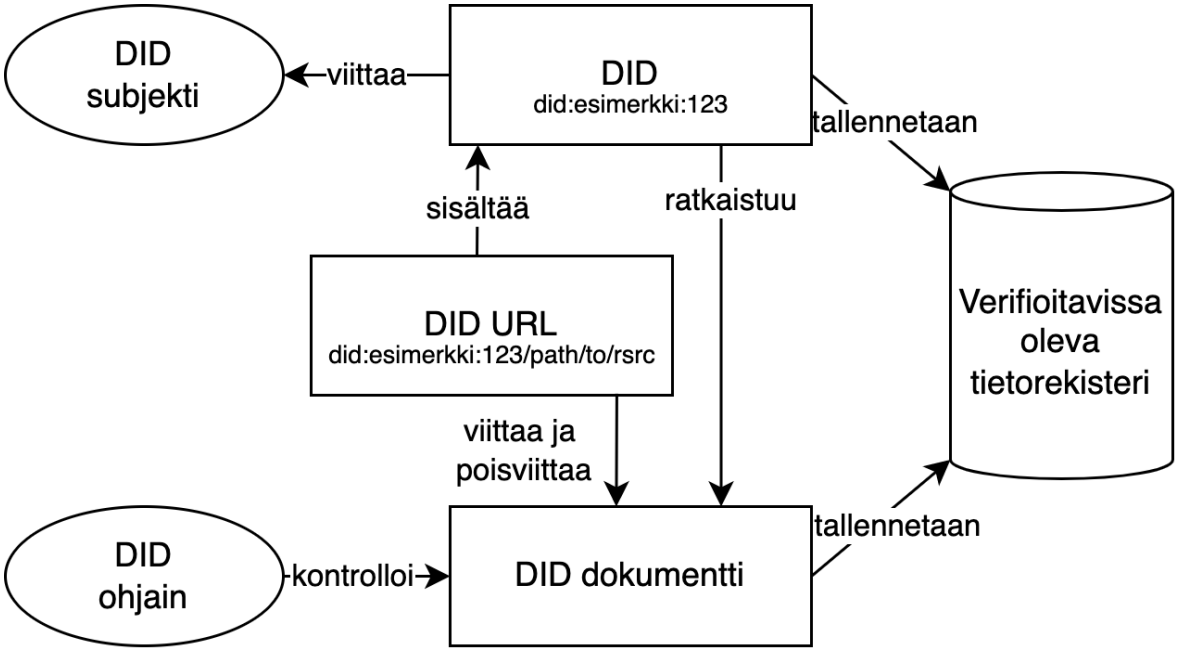
2.4.1 Hajautettu tunniste (DID)

Hajautettu tunniste (engl. Decentralized Identifier, jatkossa lyhyesti DID) on World Wide Web Consortium -organisaation (jatkossa lyhyesti W3C) (2022) kehittämä standardi tunnistautumisen toteuttamiseksi. Standardin tavoitteena on tarjota hajautettu ja verifioitavissa oleva tunniste. Kyseinen tunniste voi viivata mihin tahansa subjektiin, kuten henkilöön, organisaatioon, abstraktiin entiteettiin, datamalliin tai asiaan. Tunniste koostuu skeemasta, metodista ja metodispesifistä tunnisteesta, ks. Kuvio 3.



Kuvio 3: DID-tunnisteen osat (Sporny ym. 2022)

Osana DID-osoitetta (engl. DID-URL), edellä esitelty yhden merkkijonon tunniste viittaa DID-dokumenttiin. Tämä dokumentti sisältää DID-subjektiin liittyviä olennaisia tietoja. Näitä ovat kyseisen subjektin verifikointimenetelmä, kuten esimerkiksi kryptograafinen julkinen avain, sekä palvelut, joiden kanssa subjekti on vuorovaikutuksessa. Huomioitavaa on, että dokumentti ei kuitenkaan sisällä mitään tietoa, jota voitaisiin suoraan yhdistää subjektiin, kuten esimerkiksi nimeä tai ikää henkilön tapauksessa. Tätä dokumenttia kontrolloi DID-valvoja. Esimerkiksi tapauksessa, jolloin tunniste viittaa henkilöön, olisi DID-valvoja tavanomaisesti henkilö itse. Sekä DID-tunniste että -dokumentti tallennetaan verifioitavissa olevaan tietorekisteriin (engl. Verifiable Data Registry). Tämä on esitelty tarkemmin luvussa 2.4.4. Kuviossa 4 esitellään DID:n komponenttien välisiä vuorovaikutuksia.



Kuvio 4: DID:n komponentit ja niiden väliset vuorovaikutussuhteet (Sporny ym. 2022)

2.4.2 Todennettavat valtuustiedot

Todennettavat valtuustiedot (engl. Verifiable Credentials, jatkossa lyhyesti VC) on myös World Wide Web Consortiumin (2022) kehittämä standardi. W3C määrittelee käsitteen fyysisten valtuustietojen kautta. Fyysinen valtuustieto voi sisältää muun muassa seuraavia asioita:

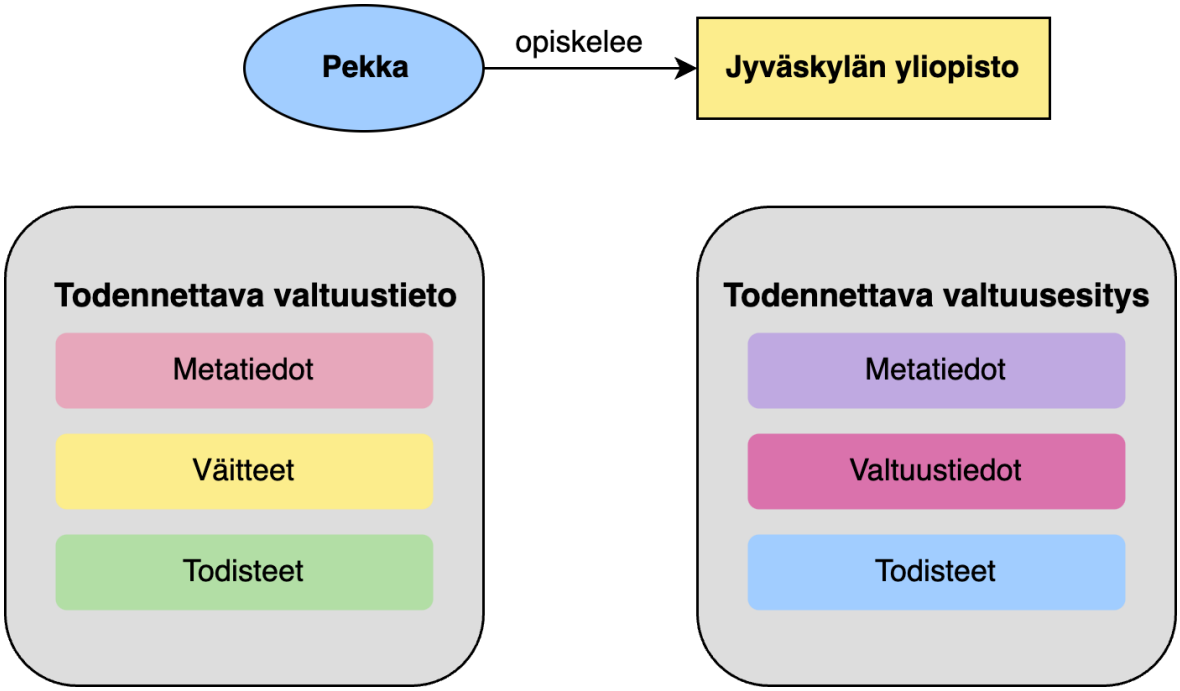
- Informaatiota valtuutettavan tunnistamiseksi (esimerkiksi kuva, nimi tai tunnus)
- Informaatiota valtuuttajasta (esimerkiksi kunnanvaltuusto tai valtio)
- Valtuuden tyyppi (esimerkiksi passi tai ajokortti)
- Muita valtuuden kannalta olennaisia tietoja, kuten sen päättymispäivä tai käytön rajoitukset

VC on digitaalinen versio näistä fyysisistä valtuustiedoista, sisältäen kaikki samat ominaisuudet kuin fyysinen vastineensa. Sen toteutuksessa hyödynnettävät teknologiat, kuten digitaalinen allekirjoitus, tekevät siitä fyysistä valtuustietoa luotettavamman. Yksi olennaisimmista konsepteista VC:hen liittyen on, miten valtuudet ovat todennettavissa. Tämä tulee esitellyksi luottamuksen kolmion -käsitteen (engl. Trust Triangle) kautta, joka käsitellään

luvussa 2.4.3.

Olennaisia käsitteitä VC:n toiminnan kannalta ovat väitteet (engl. Claims), valtuustiedot (engl. Credentials) sekä esitykset (engl. Presentations). Nämä käsitteet kulkevat edellä esitellyn järjestyksen mukaisesti VC-mallin pienimmästä osasta isoimpaan. Väitteet ovat lausuntoja subjektista, kuten esimerkiksi, että “Pekka on opiskelija Jyväskylän yliopistossa”. Valtuustieto on yhden tai useamman väitteen kokoelma yhdestä subjektista. Olennaisena osana tässä on mukana todistus siitä, että väittämät ovat tosia. Yhden valtuustiedon kaikki väittämät myöntää ja todentaa yksi taho. Valtuustieto sisältää myös sen väittämien kannalta olennaiset metatiedot.

Samaan tapaan, kuten valtuustieto on kokoelma väitteitä, esitys on kokoelma valtuustietoja. Esitys voi sisältää yhden tai useamman valtuustiedon. Kuten valtuustieto itsessään, esitys sisältää myös kokoelmalle olennaiset metatiedot ja koko kokoelman verifioivan todisteen. Mikäli valtuustietoja on vain yksi, valtuustieto itsessään muodostaa esityksen. Esitysten tarkoituksena on parantaa yksityisyyttä tarjoamalla mahdollisuus käyttäjälle esittää tietyssä tilanteessa vain haluamansa, ja sen tilanteen kannalta olennaiset, valtuustiedot kaikkien tietojen sijaan. Väitteen, valtuustiedon ja -esityksen komponentit esitellään kuviossa 5.



Kuvio 5: Väitteen, valtuustiedon ja valtuusesityksen komponentit (Sporny, Noble ja Longley 2022)

2.4.3 Luottamuksen kolmio

Valtuustietojen todentamisen mahdollistamiseksi W3C (2022) esittää käsitteet myöntäjästä (engl. Issuer), haltijasta (engl. Holder) ja todentajasta (engl. Verifier). Myöntäjä on taho, joka myöntää tietyn valtuustiedon toiselle taholle. Tämä voi olla esimerkiksi valtio, joka myöntää valtuutta auton ajamisesta, eli ajokorttia. Haltija on taho, jolle tämä valtuustieto myönnetään, tullen täten kyseisen valtuustiedon omistajaksi. Todentaja taas on taho, joka varmistaa valtuustiedon olevan tosi siinä vaiheessa, kun sitä esitetään.

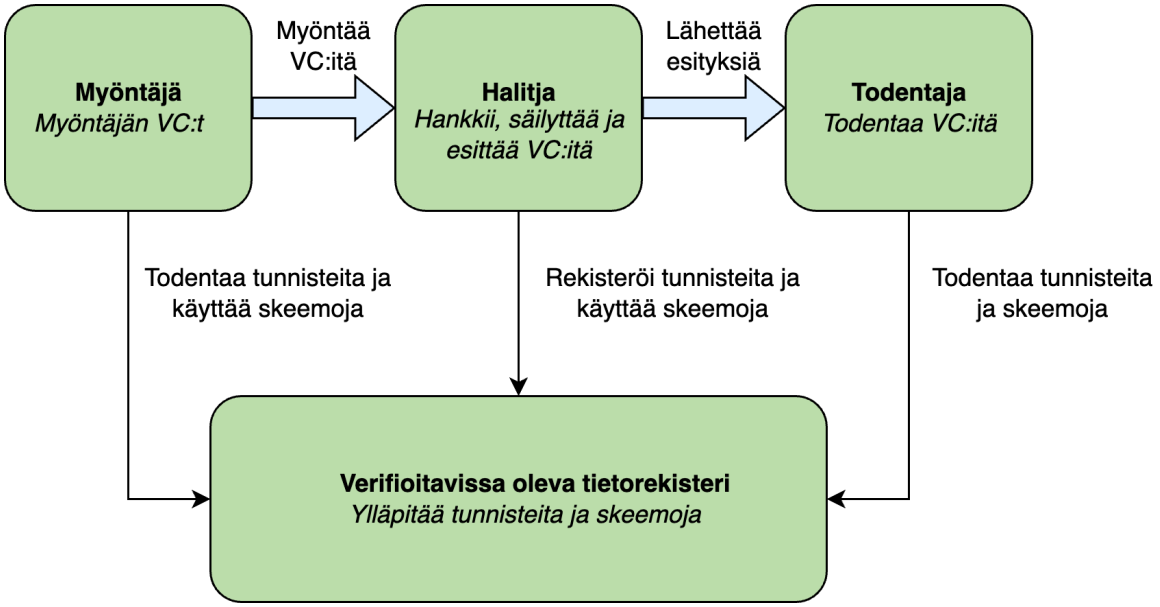
Yhdessä nämä kolme entiteettiä muodostavat keskenään mekanismin, joilla valtuustiedot verifioidaan todenmukaisiksi ja luotettaviksi. Käytämme tästä mekanismista jatkossa termiä luottamuksen kolmio (engl. Trust Triangle). Keskiössä tämän mekanismin toiminnalle on verifioitavissa oleva tietorekisteri. Kaikilla kolmella entiteetillä on oma tunniste, joka tallennetaan tietorekisteriin. Tämä tunniste yhteydessä verifioitavaan tietorekisteriin todentaa entiteetin olevan valtuutettu tekemälleen toiminnolle, kuten esimerkiksi ajokortin myöntämisen tapauksessa myöntäjäentiteetin todella olevan valtio. Kappaleessa 2.3.4 esitellään

verifioitavissa oleva tietorekisteri sekä sen toiminta luottamuksen kolmion -mekanismin kanssa.

2.4.4 Verifioitavissa oleva tietorekisteri

Verifioitavissa oleva tietorekisteri (engl. Verifiable Data Registry) on W3C:n esittämien standardien, VC:n (2022) ja DID:n (2022), yhteydessä esittämä käsite. Molemmissa näistä systeemin tarkoituksena on hallita ja pitää tallessa toimintojen kannalta olennaista dataa. Se voi olla esimerkiksi hajautettu kirjanpito (engl. distributed ledger), hajautettu levyjärjestelmä, hajautettu tietokanta tai muu luotettava datavarasto, kuten valtion tietokanta. DID:n kontekstissa tämä tarkoittaa DID-tunnisteiden tallentamista, niiden hallinnointia ja DID-dokumenttien muodostamista tunnisteista. VC:iden tapauksessa systeemi hallinnoi ja verifioi kaikkea valtuustietoihin liittyvää dataa, kuten tunnisteita, julkisia avaimia ja valtuustietojen skeemoja. Huomioitavaa on, ettei itse valtuustietoja kuitenkaan tallenneta tietorekisteriin.

Kuviossa 6 esitellään luottamuksen kolmion entiteetit ja niiden vuorovaikutukset verifioitavissa olevan tietorekisterin kanssa. Tietorekisteri on vastuussa luottamuksen kolmion luotettavasta toiminnasta. Sinne tallennetaan kaikkien kolmion entiteettien tunnisteet sekä valtuustietojen metatiedot. Näiden metatietojen, kuten myöntäjän tunnisteen sekä väitteen todistuksen, kautta sen verifioija kykenee todentamaan valtuustiedon todeksi ja voimassa olevaksi. Tietorekisteri myös mahdollistaa muun muassa valtuustietojen kumoamisen myöntäjäentiteeteille sekä niiden poistamisen haltija-entiteeteille. Tietorekisterin vuorovaikutuksia DID:n toiminnassa on havainnollistettu kuviossa 4.



Kuvio 6: Luottamuksen kolmio (Sporny, Noble ja Longley 2022)

Vaikka VC ja DID ovatkin teoriassa toisistaan irrallisia konsepteja, puhutaan niistä useimmiten toisiinsa liittyen ja yhdessä käytettävästi. Käytännössä tämä tarkoittaa DID:n hyödyntämistä VC:n eri entiteettien tunnistamisessa. VC:n standardissakin on käytetty DID-tunnisteita valtuustietojen struktuurin esimerkeissä. Sekä VC:tä että DID:tä hyödyntävässä järjestelmässä verifioitavissa oleva tietorekisteri on käytettävissä molempien käyttötarkoituksiin yhtäaikaisesti.

2.4.5 Julkisen avaimen infrastruktuuri

Julkisen avaimen infrastruktuuri (engl. Public Key Infrastructure, jatkossa lyhyesti PKI) on julkisen avaimen kryptografiaan perustuva infrastruktuuri tietoturvalliselle kommunikoinnille (Buchmann ym. 2013). PKI kehitettiin tarpeelle pystyä salaamaan kommunikaatiota kahden tahon välillä, jotka eivät olleet ennen olleet kommunikaatiossa (Ellis 1970). Tämä tarve nousi etenkin esiin internetin myötä. Ennen julkisen avaimen infrastruktuuria käytössä oli laajalti salaiseen avaimeen perustuva kryptografia. Tämä ei kuitenkaan soveltunut internetin käyttöön, sillä sen jakaminen sitä käyttävien tahojen välillä sisältää aina riskin avaimen joutumisesta vääriin käsiin. (Buchmann ym. 2013)

PKI perustuu julkisen ja yksityisen avaimen pariin. Julkinen avain on tästä parista se, joka nimensä mukaisesti jaetaan muille osapuolille. Kun viestiä ollaan lähettämässä, se salataan vastaanottajan julkisella avaimella. Tämän jälkeen viesti ei ole purettavissa millään mulla kuin vastaanottajan yksityisellä avaimella. Yksityinen avain taas on vain yhdelle taholle kuuluva avain, jota ei jaeta eteenpäin. Täten vastaanottajan saadessa viestin, hänen pitäisi pystyä luottamaan sen eheyteen ja turvallisuuteen, mikäli yksityinen avain vain ei ole vaarantunut. Pystyessä purkamaan viestin omalla yksityisellä avaimellaa, vastaanottaja samalla varmistuu siitä, että viesti on tarkoitettu juuri hänelle. (Buchmann ym. 2013)

Hajautettu julkisen avaimen infrastruktuuri (engl. Decentralized Public Key Infrastructure, jatkossa lyhyesti DPKI) on PKI:sta edelleen kehitetty malli. PKI:n käytännön hyödyntämisen mahdollistamiseksi internetiin on muodostunut kolmannen osapuolen palveluita, jotka hallinnoivat avainten määräämistä ja julkisten avainten ylläpitoa. Tämä tuo mukanaan yhden keskittyneen virhepisteen tietoturvariskin. DPKI:n tarkoituksena on eliminoida tämä riski sekä parantaa infrastruktuurin käytettävyyttä, etenkin avainten hallinnan näkökulmasta. Käytännössä DPKI mahdollistetaan hyödyntämällä hajautettua tietovarastoa, kuten esimerkiksi lohkoketjuteknologiaa. (Allen ym. 2015)

2.4.6 Hajautettu tilikirjojen teknologia

Hajautettu tilikirjojen teknologia (engl. Distributed Ledger Technology, jatkossa lyhyesti DLT) on pohjimmiltaan hajautettu tietokanta, joka koostuu fyysisesti eri paikoissa sijaitsevista tietokoneista (Liu, Farahani ja Firouzi 2020). Se ei kuitenkaan ole synonyymi hajautetulle tietokannalle. Perinteisessä hajautetussa tietokannassa kaikilla verkon jäsenillä on oikeus tehdä kaikkia CRUD-operaatiota, eli luomista, muokkaamista, lukemista ja poistamista. Tämä tuo riskin Byzantinen ongelman ilmaantumiselle eli epäjohdonmukaisuuksille tietokantojen välillä. DLT on versio hajautetusta tietokannasta, jossa oletetaan virheellisten tai korruptoituneiden solmujen eli tietokantojen olemassaolo. Yksi DLT:n pääominaisuuksista on, että siinä pelkästään lisäämis- ja lukemisoperaatiot ovat sallittuja. Kun tieto on kerran lisätty, sitä ei voi enää muokata eikä poistaa. (Sunyaev 2020)

Käytännössä DLT:n houkuttelevuus nousi lohkoketjuteknologian, tarkemmin Bitcoin-lohkoketjun,

esittelemisen myötä (Sunyaev 2020). Lohkoketju on hajautettu ja muuttumaton tilikirja transaktioiden tallentamiseen. Dataa liitetään (engl. append) jatkuvasti ja se on luettavissa kaikille verkon jäsenille. Pohjimmiltaan lohkoketju on hash-koodeilla toisiinsa yhdistetyistä lohkoista koostuva linkitetty lista, jossa jokainen lohko viittaa edelliseen lohkoon. (El Ioini ja Pahl 2018)

Lohkoketjuja on kahden tyyppisiä: avoimia (engl. permissionless) ja suljettuja (engl. permissioned). Avoimiin lohkoketjuihin voi liittyä kuka tahansa ilman erillistä hyväksyntäprosessia. Suljetut lohkoketjut jaottuvat edelleen kahteen: federoituihin ja yksityisiin. Federoidussa lohkoketjun hallinnassa on joukko erikseen valittuja tahoja. Yksityisessä tämä taas on yksi taho, useimmiten jokin organisaatio. Molemmissa tapauksissa lohkoketjun lukeminen voidaan tehdä avoimeksi, mutta kirjoittaminen ja ketjun validointi on rajoitettua. (Liu, Farahani ja Firouzi 2020) Kaikille tyypeille olennainen osa on lohkoketjun konsensus mekanismi (engl. consensus mechanism) eli menetelmä päättää, mitä lohkoja ketjuun lisätään (El Ioini ja Pahl 2018). Näitä on monia erilaisia ja eri tarkoituksiin, mutta kaksi tunnettua ja paljon käytettyä mekanismia ovat Proof-of-Work- ja Proof-of-Stake-algoritmit (Liu, Farahani ja Firouzi 2020).

Toinen teknologia, jolla DLT voidaan toteuttaa, on suunnattu asyklinen graafi (engl. Directed Acylic Graph, jatkossa lyhyesti DAG) (Liu, Farahani ja Firouzi 2020; El Ioini ja Pahl 2018). Olennaisin ero DAG:n ja lohkoketjujen välillä on viittauksien suunta sekä transaktioiden validointimenetelmä. DAG:ssa solmut eli transaktiot viittaavat uuteen, eli seuraavaan solmuun, kun taas lohkoketjussa uutta transaktiota luodessa viitataan edelliseen solmuun. Samanaikaisesti luodessaan viittaukset edellisiin transaktioihin, uusi transaktio DAG:ssa validoi edelliset transaktiot. Tästä syystä DAG:ssa ei ole käsitettä louhimisesta, joka on lohkoketjujen tapa validoida uusia transaktioita. DAG ei myöskään sisällä käsitettä lohkoista. (Liu, Farahani ja Firouzi 2020)

2.4.7 Älysopimukset

Älysopimus (engl. Smart Contract) esiteltiin jo vuonna 1994 ja se määriteltiin silloin seuraavasti: “tietokoneistettu transaktioprotokolla, joka täyttää sopimuksen ehdot”. Yleisesti

älysopimus on tietokoneohjelma, jonka tarkoituksena on automaattisesti toteuttaa, valvoa tai dokumentoida tapahtumia sopimuksen neuvottelussa tai suorittamisessa digitaalisesti. (Christidis ja Devetsikiotis 2016).

Älysopimuksista puhutaan SSI:n kontekstissa kuitenkin lohkoketjujen yhteydessä. Silloin ne ovat lohkoketjuun tallennettuja ohjelmia, jotka ajetaan, kun tietyt ennalta määrätyt ehdot täyttyvät. Niitä käytetään monimutkaisempien transaktioiden toteutukseen joustavilla ja ohjelmoitavilla menetelmillä. (Saidi ym. 2022; Song ym. 2020) Yang ja Li (2020) lisäävät myös, että älysopimukset toimivat omatoimisesti ja eivät tarvitse kolmatta osapuolta toimiakseen. Älysopimukset luodaan ja ajetaan siten, että yksiköt lähettävät transaktioita, mikä estää sääntöjen yksipuolisen peukaloinnin. Niiden avulla myös julkistetaan yksittäisen entiteetin toimintaprosessi, ja lohkoketjun taustalla oleva konsensusmekanismi takaa transaktioiden tulosten oikeellisuuden ja johdonmukaisuuden. (Yang ja Li 2020) Kun Älysopimus on julkaistu lohkoketjuverkossa, sen sisältö on lähes muuttumaton, sillä jokaisella verkon solmulla on sama kopio sopimuksesta (Lesavre ym. 2019).

2.4.8 Tietovarasto

Tietovarastosta (engl. Data Storage) puhuttaessa voidaan tarkoittaa mitä tahansa paikkaa, johon voidaan tallentaa tietoa. Käytännössä tämä tarkoittaa jotakin levyä jollakin tietokoneella. Mühle ym. (2018) esittävät tietovaraston jakautuvan SSI:n kontekstissa kahteen: julkiseen varastoon ja yksityiseen varastoon. Julkiseen varastoon heidän mukaansa kuuluu kaikki tieto, joka on kaikkien luettavissa. Julkisesti tallennettavaa tietoa on lähtökohtaisesti kaikki verifioitavissa olevaan tietorekisteriin tallennettu tieto, muun muassa DID:t. Julkiseen tietovarastoon voidaan teoriassa tallentaa mitä vain käyttäjän preferensseistä ja SSI:n käytännön toteutuksesta riippuen, mutta kaikki julkisesti tallennetulla tiedolla on riski vaarantua (Mühle ym. 2018).

Vastaavasti yksityisellä tietovarastoon tallennettu tieto on sitä, mikä ei ole muille, kuin tiedon omistajalle saatavilla. Tähän kuuluu etenkin VC:t sekä DID:hen linkitetty yksityinen avain (Mühle ym. 2018; Dib ja Toumi 2020). Tämä voi olla käyttäjän oma laite, kuten puhelin tai tietokone, tai luotetun kolmannen osapuolen palvelu (Dib ja Toumi 2020). Mühle

ym. (2018) esittävät omalle laitteelle tallentamisen antavan täyden kontrollin käyttäjälle ja poistavan tarpeen kolmanteen osapuoleen luottamiseen, mutta olevan ongelmallinen datan häviämisen tai varkauden tapauksissa.

Lokaalille laitteelle tallentaminen ei kuitenkaan ole ainut tapa toteuttaa yksityistä tietovarastoa SSI:ssä. Monilla tämänhetkisillä SSI:n toteutuksilla on oma tapansa toteuttaa yksityinen tietovarasto. UPort hyödyntää yksityisen tiedon varastointiin IPFS-teknologiaa (The InterPlanetary File System) (Lundkvist ym. 2016). Se on hajautettu vertaisverkkotiedostojärjestelmä, joka perustuu hajautettuun "hash table" -tekniikkaan (Benet 2014). Blockstack hyödyntää keskitettyjä varastointipalveluita, kuten Amazon S3:n, Google Drive ja Dropboxin, muodostaen niistä yhdessä hajautetun tapaisen tietovaraston (Ali ym. 2016). ShoCard taas toteuttaa varastoinnin keskitetysti, mutta pyrkii säilyttämään yksityisyyden salaamalla datan "kryptografisia hasheja" käyttäen, jotka vain datan omistaja voi purkaa (Shuaib, Hassan, Usman, Alam, Bhatia, Agarwal ym. 2022). Sovrin puolestaan toteuttaa ensimmäisenä esiteltyä tapaa eli käyttäjien yksityinen data tallentuu vain heidän omille laitteilleen lokaalisti (Windley ja Sovrin 2018). Kaikissa näistä on omat hyvät ja huonot puolensa. Pääasiassa tasapainottelu tapahtuu käytettävyyden ja käyttäjän yksityisyyden välillä.

2.4.9 Digitaalinen lompakko

Yleisesti puhuttuna digitaalinen lompakko (engl. Digital Wallet) on samankaltainen kuin fyysisen maailman lompakkokin (Jing ym. 2021). Teknologian kehityksen myötä älypuhelimia voidaan nykyään käyttää rahansiirtoon tai maksamiseen puhelimiin asennettujen sovellusten avulla. Maksamisen lisäksi ihmiset voivat tallentaa puhelimiinsa muun muassa kuitteja, kuponkeja, käyntikortteja ja laskuja. Kun älypuhelinta voidaan käyttää kuin normaalia nahkalompakkoa, sitä kutsutaan "digitaaliseksi lompakoksi". (Rathore 2016) Digitaalista lompakkoa siis säilytetään älypuhelimessa, tai oikeastaan älypuhelin on nykyään digitaalinen lompakko.

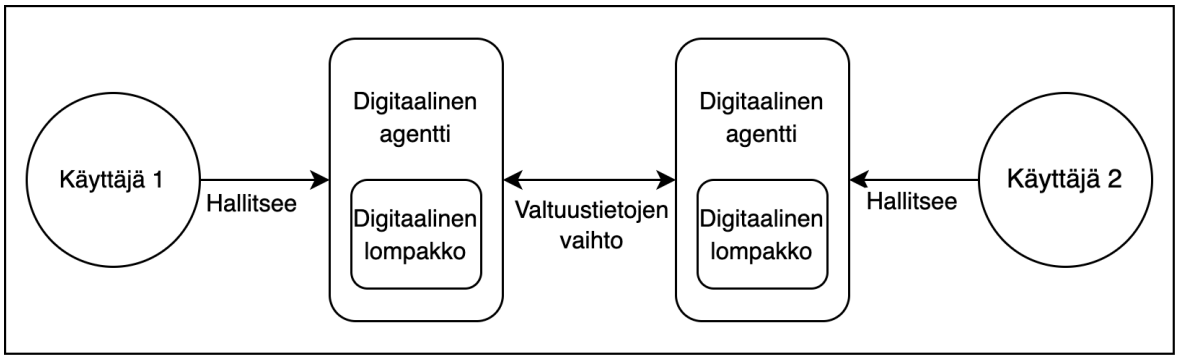
Tässä tutkimuksessa digitaalista lompakkoa käsitellään SSI:n näkökulmasta. Tällöin digitaalisella lompakolla on oltava enemmän toimintoja. Yksinkertaisesti tässä kontekstissa digitaalinen lompakko on sovellus, johon tallennetaan yksityiset avaimet, VC:t ja DID:t (D.

Pöhn, M. Grabatin ja W. Hommel 2021). Jing ym. (2021) väittää, että ensinnäkin, koska itsehallittavan identiteetin vuorovaikutus on vertaisten välistä vuorovaikutusta, se voi tapahtua hyvin monimutkaisissa ja muuttuvissa sovellusskenaarioissa, joten lompakossa on säilytettävä tunnistetietoja, jotka ovat yhteensopivia eri standardien, formaattien ja toimintojen kanssa. Toiseksi, lompakko on oltava synkronoitavissa erilaisiin toimintaympäristöihin, aivan kuten voimme halutessamme laittaa rahat mihin tahansa vaatteiden taskuun. Kolmantena, valtuustiedot tulee pystyä siirtämään lompakosta toiseen. Käyttäjät voivat vapaasti poistaa valtuustiedot yhdestä lompakosta ja siirtää ne toiseen lompakkoon täyttääkseen sovelluksen vaatimukset erilaisissa skenaarioissa. Digitaalisen lompakon tehtävä on siis säilyttää yhtenäisesti erilaisia tunnistetietoja, säilyttää julkisia avaimia, suojata tunnistetietoja varkauksilta ja helpottaa käyttöä. Käyttäjät voivat samaan aikaan hallita useita elektronisia laitteita, kuten matkapuhelimia ja henkilökohtaisia tietokoneita. (Jing ym. 2021)

Shuaib, Hassan, Usman, Alam, Bhatia, Agarwal ym. (2022) mukaan digitaalinen lompakko suojaa haltijan käyttöoikeuksia varmistamalla, että vain valtuutetuilla henkilöillä on pääsy lompakkoon. Se myös turvaa ja suojaa tiedot salauksen avulla. Lisäksi se todentaa DID-asiakirjojen siirrot ja niiden kryptografiset todisteet. Se tarjoaa myös mekanismin, jonka avulla yksilöt voivat päivittää valtuustietonsa. Valtuustietojen tallentamiseen ja hallintaan liittyen digitaalista lompakkoa voi käyttää myös valtuustietojen palautukseen, jos lompakko katoaa tai salasanat vaarantuvat. Palautusmenetelmät on kuitenkin oltava otettu käyttöön ennakkoon. Esimerkiksi pilvipalvelua hyödyntävissä varmuuskopioissa tai muissa lompakon tarjoajan mahdollistamissa varmuuskopioissa olisi kuvattava, miten tai milloin käyttäjät voivat hakea tunnistetiedot. Täytyy kuitenkin muistaa, että valtakirjojen palautusprosessin on oltava tasapainossa käytettävyyden ja turvallisuuden kanssa. (Shuaib, Hassan, Usman, Alam, Bhatia, Agarwal ym. 2022)

Digitaalisesta lompakosta puhuttaessa mainitaan usein myös digitaaliset agentit. Nämä agentit ovat ohjelmia digitaalisissa lompakoissa, jotka vastaavat lompakon turvallisuudesta, osallistuvat turvalliseen valtuustietojen vaihtoon ja muodostavat yhteyksiä hajautetun sekä turvallisen viestitysprotokollan kautta. (P. Bai ym. 2022) Digitaaliset agentit siis kehittävät, käyttävät ja ylläpitävät digitaalista lompakkoa (D. Pöhn, M. Grabatin ja W. Hommel 2021; Jing ym. 2021). Tämän lisäksi digitaaliset agentit toimivat vertaisverkkoyhteyksien

luojina (ks. kuvio 7). Saatuaan käyttäjältä käskyn, digitaalinen agentti muodostaa yhteyden toisen osapuolen digitaaliseen agenttiin verkossa ja muodostaa vuorovaikutteisen yhteyden. Käyttäjä suorittaa digitaalisen identiteetin tarkistuksen ja valtuustietojen keskustelun toisen osapuolen kanssa hajautetun ja salatun tiedonvaihtoprotokollan kautta. (Jing ym. 2021) Reuna-agentit (engl. Edge-agent) ja pilviagentit ovat kaksi digitaalisen agentin yleistä kategoriaa (P. Bai ym. 2022).



Kuvio 7: Digitaalisten agenttien vertaisverkkoyhteyden muodostus (Jing ym. 2021)

2.4.10 Nollatietotodiste

Nollatietotodiste (engl. zero-knowledge proof) on digitaalinen menetelmä, jossa yksi osapuoli todistaa toiselle osapuolelle (esim. käyttäjä palveluntarjoajalle), että hänellä on jotain tietoa hallussaan paljastamatta tämän tiedon sisältöä. Näin ollen todelliset arvot pysyvät suojattuina, mutta esimerkiksi palveluntarjoaja voi silti varmistaa joitakin käyttäjää koskevia tietoja (Dib ja Toumi 2020; Saidi ym. 2022; Lesavre ym. 2019). Nollatietotodisteen ansiosta käyttäjän on myös mahdollista jakaa itsestään vain vaadittava minimimäärä tietoa (Stokkink ja Pouwelse 2018). Esimerkiksi, jos käyttäjän täytyy todistaa olevansa yli 21-vuotias, sen sijaan, että todentajalle lähetettäisiin todellinen syntymäaika, voidaan lähettää väite “ikä on yli 21 vuotta”, joka on kryptografisesti todennettavissa. Tämän tyyliset tiedonvaihdot säilyttävät käyttäjän yksityisyyden ja estävät todentajaa mahdollisesti esiintymästä identiteetin omistajana. (Soltani, Nguyen ja An 2021)

López (2020) mukaan nollatietotodisteiden yleisimmät muodot ovat seuraavat:

- **Tasa-arvoisuus tai ei-tasa-arvoisuus**: Suureen arvo on yhtä suuri tai ei yhtä suuri

kuin tietty arvo. Esim. Onko henkilö tietyn ikäinen?

- **Eriarvoisuus**: Suureen arvo on suurempi tai pienempi kuin annettu arvo. Esim. Ylittääkö tilin saldo maksettavan summan?
- **Jäsenyys**: Kohde on listalla. Esim. Onko kohde jonkin seuran jäsen?
- **Vaihteluväli**: Suureen arvo on tai ei ole tietyn aikavälin sisällä. Esim. Onko kaupan kävijämäärä 0 - 50 hengen välillä?

Nollatietotodisteessa esiintyy yleensä todistaja (engl. Prover) joka yrittää todistaa väitteen paikkansapitävyyden ja todentaja (engl. Verifier), joka yrittää todentaa, onko väite totta (Lesavre ym. 2019; López 2020). Lesavre ym. (2019) mukaan nollatietotodisteen pitäisi täyttää seuraavat kolme ominaisuutta:

- **Aukottomuus** (engl. Completeness): Jos väite pitää paikkansa, rehellinen todentaja on vakuuttunut.
- **Oikeellisuus** (engl. Soundness): Jos väite on väärä, huijaavan todistajan ei ole mahdollista vakuuttaa todentajaa.
- **Nollatieto** (engl. Zero-knowledge): jos väite pitää paikkansa, todentaja ei saa mitään muuta selville, kuin että tieto pitää paikkansa.

3 Tutkimusmenetelmä

Tässä luvussa käydään läpi tutkielman tutkimusmenetelmät. Aluksi käsitellään tutkimuksen motivaatio. Tämän jälkeen esitellään kumpaankin tutkimukseen liittyvät taustatiedot, jonka jälkeen taas molempien tutkimuksien prosessit tässä tutkielmassa. Lopuksi pohditaan molempien tutkimusten validiutta kokonaisuudessaan.

3.1 Motivaatio

Tämä tutkielma koostuu kahdesta tutkimuksesta: systemaattisesta kirjallisuuskartoituksesta sekä kyselytutkimuksesta. Kirjallisuuskartoituksen avulla etsittiin vastausta tutkimuskysymyksiin: “Mikä on itsehallittavan identiteetin määritelmä ja mitkä ovat sen tärkeimmät komponentit?” ja “Mitä potentiaalisia hyötyjä ja haasteita itsehallittavaan identiteettiin liittyy käyttäjän näkökulmasta?” Kyselytutkimuksen tavoitteena taas oli etsiä vastausta tutkimuskysymykseen: “Mitkä ovat olennaisimmat itsehallittavan identiteetin hyödyt ja haasteet Suomen digitaalisen henkilöllisyystodistuksen kontekstissa loppukäyttäjän näkökulmasta?” Tutkielma suoritettiin laajempana kaksiosaisena kokonaisuutena, sillä siten saatiin vastaus kaikkiin tutkimuskysymyksiin. Eri tutkimuskysymyksiin vastaamisen lisäksi systemaattinen kirjallisuuskartoitus toimi pohjana kyselytutkimukselle.

Tutkielman ensimmäinen tutkimuksen, eli systemaattinen kirjallisuuskartoituksen tavoitteena oli selvittää SSI:n määritelmää, sen keskeisiä komponentteja sekä siihen liittyviä potentiaalisia hyötyjä ja haasteita. Motivaationa näiden tutkimiseen oli se, ettei niitä ollut vielä tutkittu systemaattisesti eikä riittävästi ylipäänsä. Näistä potentiaalisten hyötyjen ja haasteiden tutkimisen toisena olennaisena motiivina oli tuloksien hyödyntäminen seuraavassa tutkimuksessa. Systemaattisessa kirjallisuuskartoituksessa selvinneet tulokset pohjustivat kyselytutkimuksen kysymyksiä.

Jälkimmäinen tutkimus toteutettiin kyselytutkimuksena. Tämän osion tavoitteena oli selvittää loppukäyttäjien näkemyksiä Suomen digiuudistuksesta. Olennaisimpina tutkimuskohteina oli tarkastella, mitkä hyödyt loppukäyttäjät kokivat tärkeimpinä ja mitkä haasteet uhkaavimpina. Samaan tapaan tavoitteena oli myös käänteisesti selvittää, mitkä ovat hyödyt

koettiin vähiten tärkeiksi ja mitkä haasteet vähiten uhkaaviksi.

3.2 Taustatieto

Aluksi taustatieto-osiossa puhutaan tutkimusten toteutuksesta ja sen osioista yleisesti. Sen jälkeen esitellään systemaattisen kirjallisuuskatsauksen (Kitchenham ja Charters 2007) sekä -kartoituksen (Petersen ym. 2008) menetelmät ja näiden pohjalta johdettu tämän tutkimuksen menetelmä systemaattiseen kirjallisuuden toteuttamiseen. Luvussa määritellään myös määrälliset ja laadulliset tutkimusmenetelmät sekä käydään läpi kyselytutkimuksen toteutukseen liittyvät vaiheet ja esitiedot.

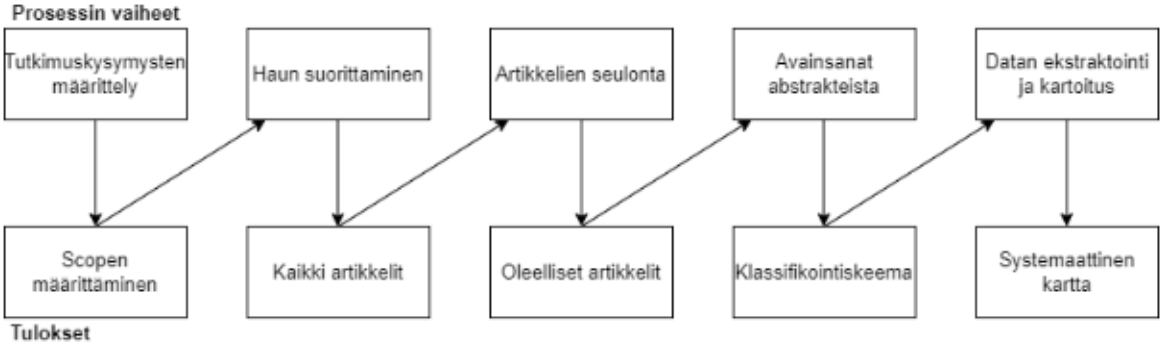
3.2.1 Systemaattinen kirjallisuuskartoitus

Systemaattinen kirjallisuuskatsaus (engl. Systematic Literature Review) on tapa identifioida, arvioida ja tulkita kaikkea saatavilla olevaa relevanttia tutkimusta tietystä aihealueesta tai kiinnostuksen kohteesta (Kitchenham ja Charters 2007). Siinä tarkastellaan primääritutkimuksia perusteellisesti ja kuvaillaan niiden metodologiaa sekä tuloksia (Petersen ym. 2008). Systemaattisella kirjallisuuskatsauksella on huomattavia etuja perinteiseen kirjallisuuskatsaukseen verrattuna, kuten esimerkiksi pienempi todennäköisyys tulosten puolueellisuudelle ja vääristymille sekä eri tutkimusasetelmien laajempi tarkastelu (Kitchenham ja Charters 2007). Kitchenham ja Charters (2007) esittävät seuraavat vaiheet systemaattisen kirjallisuuskatsauksen suorittamiseen:

1. Katsauksen tarpeen identifiointi
2. Katsauksen pyytäminen (vapaavalintainen)
3. Tutkimuskysymysten määrittely
4. Hakuprotokollan kehittäminen
5. Hakuprotokollan arviointi (vapaavalintainen)
6. Tutkimuksen identifiointi
7. Primääritutkimusten valinta
8. Tutkimuksen laadunarviointi
9. Datan ekstraktointi ja monitorointi

10. Datan analysointi
11. Datan esittämisen strategia
12. Raportin toteuttaminen
13. Raportin arviointi (vapaavalintainen)

Systemaattinen kirjallisuuskartoitus (engl. Systematic Mapping Study) tarjoaa struktuurin tietystä aihepiiristä tehdyistä tutkimuksista kategorisoimalla ne. Tavanomaisesti saadut tulokset (kategoriat) esitetään jossain visuaalisessa muodossa (Petersen ym. 2008). Se tarjoaa yleisen katsauksen tietystä tutkimuskohteesta ja toimii hyvin pohjana spesifimmälle kirjallisuuskatsaukselle (Kitchenham ja Charters 2007). Petersen ym. (2008) esittävät systemaattiselle kirjallisuuskartoitukselle seuraavat vaiheet:



Kuvio 8: Kirjallisuuskartoituksen prosessi (Petersen ym. 2008)

Systemaattisen kirjallisuuskartoituksen ja -katsauksen prosessit ovat monilta osin hyvin samankaltaiset. Molemmissa menetelmissä hakusanojen ja -kriteerien suunnittelu sekä hakuprosessin toteuttaminen suoritetaan systemaattisesti. Molemmissa niistä esiintyvät tämän myötä systemaattisen prosessin tuomat edut perinteiseen kirjallisuuskatsaukseen verrattuna (Kitchenham ja Charters 2007; Petersen ym. 2008). Niillä on kuitenkin myös selviä eroja toisiinsa verrattuna. Yhtenä näistä on jo mainittu artikkelien tarkastelun perusteellisuus. Systemaattisella kirjallisuuskartoituksella pyritään tavanomaisesti vastaamaan suurpiirteisempiin tutkimuskysymyksiin ja niitä voi myös olla useampi. Tästä syystä systemaattisella kirjallisuuskartoituksella on mahdollisuus myös tarkastella suurempaa joukkoa aineistoa (Kitchenham ja Charters 2007).

Tarkasteltavassa aineistossa voi myös olla eroa. Systemaattisessa kirjallisuuskatsauksessa

tarkastellaan tavanomaisesti vain empiiristä aineistoa ja pyritään tämän kautta selvittämään kohteesta olemassa olevan tiedon nykytilaa. Systemaattisessa kirjallisuuskartoituksen päätavoite tietyn aihepiirin tutkimusten luokittelusta taas sallii muunkin kuin empiirisen tutkimuksen tarkastelun (Petersen ym. 2008).

Tässä tutkimuksessa suoritettiin systemaattinen hakuprosessi, joka mukailee molempia edellä esitetyistä menetelmistä. Tarkastellun kirjallisuuden määrä viittaa enemmän systemaattiselle kirjallisuuskartoitukselle tyypilliseen aineiston määrään. Tutkimuksen päätavoitteena ei kuitenkaan ollut tehdä systemaattista karttaa aineiston luokittelemiseksi, vaikka myös luokittelua toteutettiin muun muassa tutkimuskohteiden pohjalta. Tutkimuskysymyksiin vastaamiseksi ainestoa myös tarkasteltiin perusteellisemmin artikkelien koko tekstin osalta, viitaten enemmän systemaattisen kirjallisuuskatsauksen datankeruuprosessiin. Toisaalta suurin osa tutkimuksen aineistosta oli ei-empiiristä tutkimusta, täten poiketen systemaattiselle kirjallisuuskatsaukselle tyypillisestä tarkastelukohteesta. Vaikka prosessi sisälsi elementtejä molemmista esitellyistä menetelmistä, kallistuu tutkimus enemmän systemaattisen kirjallisuuskartoituksen puolelle. Käytämme jatkossa siis termiä “systemaattinen kirjallisuuskartoitus” tutkimusmenetelmän kuvaamiseen.

3.2.2 Kyselytutkimus

Tässä tutkimuksessa käytetään sekä määrällisiä että laadullisia tutkimusmenetelmiä. Määrällisellä tutkimuksella on kuitenkin selkeä pääpaino tässä tutkimuksessa. Laadullista tutkimusta käytetään vain täydentävänä tutkimusmuotona.

Määrällinen tutkimusmenetelmä eli kvantitatiivinen menetelmä on tutkimustapa, jossa tietoa tarkastellaan numeerisesti. Sen tarkoituksena on selittää, kuvata, kartoittaa, vertailla tai ennustaa ihmistä koskevia asioita tai luonnon ilmiöitä numeraalisesti. Määrällisessä tutkimuksessa pyritään löytämään aineistosta säännönmukaisuuksia matemaattisia menetelmiä hyödyntäen. (Vilkka 2007).

Tämän tutkimuksen aineistonkeruumenetelmäksi valikoitui kyselytutkimus, joka on yksi tapa toteuttaa määrällistä tutkimusta (Creswell 2014). Kyselytutkimus on informaation keräämistä, joka pohjautuu tietyn otoksen vastauksista tiettyihin kysymyksiin. Se on tehokas

tapa kerätä dataa systemaattisesti laajalta valikoimalta eri taustoja omaavilta yksilöiltä. Kyselytutkimuksessa voidaan myös mitata useampia muuttujia ilma, että käytetty aika nousee suuresti. (Check ja Schutt 2012) Vilkka (2007) sanoo kyselytutkimuksen olevan sopiva menetelmä, kun havaintoyksikkönä on henkilö ja häntä koskevat asiat, kuten mielipiteet, asenteet, ominaisuudet tai käyttäytyminen. Hän myös mainitsee sen soveltuvan tilanteisiin, jossa tutkittavia on paljon ja ne ovat hajallaan.

Vastauksia kyselytutkimukseen kerätään käyttämällä lomaketta, joka voidaan jakaa postitse tai verkkokyselynä (Vilkka 2007). Verkkokyselyn etuna postitse lähettämiseen on kustannustehokkuus ja korkeampi mahdollisuus saavuttaa laaja otanta (Lefever, Dal ja Matthıasdóttir 2007). Näistä syistä kyselyn jakamiseen valikoitui tässä tutkimuksessa verkkokysely.

Kyselytutkimuksen onnistuneeseen toteuttamiseen liittyy tiettyjä asioita, joita tutkijan on syytä ottaa huomioon. On tärkeää huomioida, että kyselyn suunnittelu ja toteutus vaatii huolellisuutta, ettei se tuota harhaanjohtavia tuloksia. Tämä esiintyy etenkin kysymysten suunnittelussa. Kysymysten tulisi olla selkeitä ja käyttää mahdollisimman ymmärrettävää kieltä. Kysymykset tulisi myös muodostaa niin, etteivät ne herätä vastaajassa mitään tunteita. Kysymykset eivät myöskään saa olla johdattelevia. Yleisesti kysymysten tulisi olla mahdollisimman neutraaleja niin, että kaikki vastaajat kokevat ja ymmärtävät kysymykset samalla tavalla. (Neuman 2014) Näitä asioita pyrittiin huomioimaan kyselyn suunnittelussa ja toteutuksessa.

3.3 Systemaattinen kirjallisuuskartoitus

Tämä luku käsittelee systemaattisen kirjallisuuskartoituksen prosessia. Luvussa käydään läpi, miten kartoituksessa on toteutettu hakusanojen ja valintakriteerien muodostus, datan kerääminen ja tallentaminen. Lopuksi vielä pohditaan, miten tulosten analysointi toteutettiin.

3.3.1 Tietokannat ja hakulausekkeet

Tietolähteen valinnan suhteen tutkimuksessa päädyttiin käyttämään Scopus-tietokantaa. Aluksi tarkoituksena oli käyttää tietokantana Scopuksen lisäksi myös Google Scholaria, mutta se ei ollut mahdollista tälle tutkielmalle varatun ajan puitteissa. Scopuksesta löytyneet tulokset olivat myös alustavien hakujen perusteella riittävän kattavia tutkimusta varten.

Hakulausekkeen määrittely alkoi yksinkertaisilla lausekkeilla “digital identity”, “self-sovereign” ja “SSI”, jotta saataisiin kuvaa siitä, miten paljon tuloksia tulee ja millaisia tulokset ovat. Tämän jälkeen hakulausekkeeseen lisättiin erilasia spesifimpiä hakutermejä sekä testailtiin erilaisia loogisia ehtoja, kuten AND ja OR. Lopputuloksena oli melko pitkä ja monimutkainen hakulauseke. Tämän jälkeen hakulauseke yksinkertaistettiin helposti luettavaan muotoon, sillä huomattiin, että yksinkertainen muoto antaa lähes samat hakutulokset aiempaan verrattuna, jättäen pois vain epärelevantteja artikkeleita. Esiin nousi myös huomio etteivät ennen vuotta 2018 julkaistut artikkelit olleet relevantteja tutkimukseen liittyen, koska tutkimuksen aihe on niin uusi. Tästä syystä hakuehtoihin lisättiin, että hakuun sisällytetään vain vuoden 2018 jälkeen julkaistut artikkelit. Hakulausekkeen kehitys esitetään on esitelty liitteessä B. Lopulliseksi hakulausekkeeksi muodostui seuraava: “decentralized identity” OR “self-sovereign identity” OR “distributed identity”. Lopulliset haut suoritettiin 17.10.2022.

3.3.2 Valintakriteerit

Tärkeimpinä valintakriteereinä kartoituksessa olivat itsehallittavan identiteetin määritelmän sekä hyötyjen ja haasteiden esiintyminen. Nämä kriteerit nähtiin tärkeimmiksi, koska ne olivat suoraan liitoksissa tutkimuskysymyksiin vastaamiseen. Toinen hyväksymiskriteeri käsitteli artikkelin tutkimuksen menetelmää. Artikkeleita myös hylättiin julkaisun tyypin, julkaisuvuoden, kielen ja saatavuuden mukaan.

Tutkimuksessa käytetyt valintakriteerit olivat seuraavat:

Hyväksymiskriteeri 1 (vähintään yksi täyttyy)

1. Esittää itsehallittavan identiteetin määritelmän
2. Esittää itsehallittavan identiteetin tuomia hyötyjä tai siihen liittyviä haasteita käyttä-

jän näkökulmasta

Hyväksymiskriteeri 2 (vähintään yksi täyttyy)

1. On empiirinen tutkimus, jonka pääasiallisena tutkimuskohteena on SSI
2. Esittää uuden mallin/ehdotuksen (engl. proposal), jonka pääkomponenttina on SSI
3. Kirjallisuuskatsaus tai -kartoitus SSI:n aihepiiriin

Hylkäämiskriteerit (mikäli yksi täyttyy)

1. Kirja tai sen kappale
2. Ennen vuotta 2018 julkaistu
3. Ei ole alkuperäisartikkeli
4. Ei ole englanninkielinen
5. Artikkeli ei ole kokonaisuudessaan saatavilla

3.3.3 Aineiston hallinta

Aineiston hallintaa varten luotiin Google Sheets -dokumentti, johon tallennettiin kaikki kartoitukseen liittyvä data. Tähän dokumenttiin suoritettiin sekä artikkelien seulonta, että varsinainen datankeruu. Dokumenttiin tallennettiin kaikista artikkeleista perustiedot, kuten julkaisuvuosi, nimi, julkaisijoiden nimet ja lyhyt tiivistelmä artikkelista.

Artikkelien seulontaan liittyen lisättiin sarake kuvaamaan, onko artikkeli hylätty otsikon tai abstraktin perusteella, hylätty koko tekstin perusteella vai hyväksytty kartoitukseen. Tämän lisäksi lisättiin sarake hylätyille artikkeleille, johon kirjoitettiin hylkäämisen syy, sekä hyväksytyille, johon kirjoitettiin täyttyneet valintakriteerit, eli hyväksymisen peruste. Datankeruun osalta dokumenttiin tallennettiin kerättävään dataan liittyvät tiedot, kuten itsehallittavan identiteetin määritelmä viittauksineen ja tärkeimpine komponentteineen sekä artikkelissa esitetyt mahdolliset hyödyt ja haasteet liittyen itsehallittavaan identiteettiin. Tämän lisäksi tallennettiin myös artikkelin tutkimuskohde sekä siinä käytetty tutkimusmenetelmä, mikäli tämä oli mainittu. Dokumenttiin kerättiin myös muita ylimääräisiä tietoja tutkijoiden töiden helpottamiseksi.

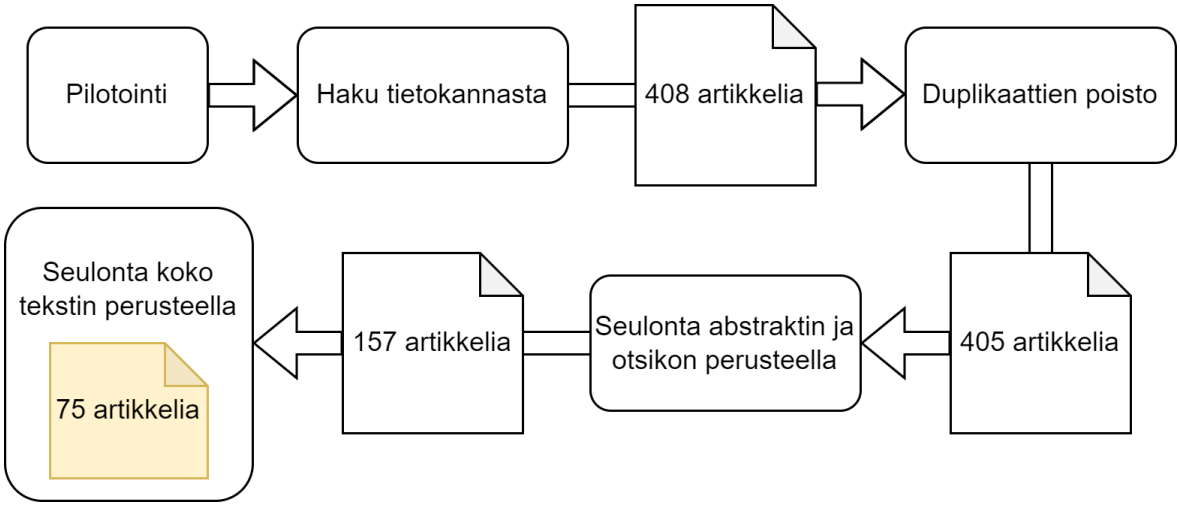
3.3.4 Pilotointi

Pilotoinnin tarkoituksena oli suorittaa kartoitusprosessi pienemmällä otannalla, jotta saataisiin selville, toimivatko hakusanat ja valintakriteerit halutulla tavalla. Tarkoituksena oli myös saada selville, saadaanko tuloksia sopiva määrä. Pilotointi alkoi ennakkotyöllä, jossa määriteltiin hakusanoja ja valintakriteerejä abstraktien perusteella. Tätä iteroitiin useampien hakujen kautta, josta tarkempi raportti esitettiin taulukossa **??**. Lopullisen hakusanojen lukitsemisen jälkeen tuloksia löytyi 408. Ennen lopullista pilotointia artikkeleita luettiin vielä abstraktien ja otsikoiden, ja osittain koko tekstien, perusteella, jotta valintakriteerit saatiin hiottua lopulliseen muotoonsa.

Kun valintakriteerit oli saatu lopulliseen muotoon, suoritettiin lopullinen pilotointi. 408:stä artikkelista valittiin sattumanvaraisesti 100 artikkelia tarkasteltavaksi abstraktien ja otsikon perusteella. Näistä artikkeleista 42 läpäisi valintakriteerit ja loput hylättiin. Hyväksyttyjen artikkelien suhde hylättyihin vaikutti sopivalta ja valintakriteerit toimivilta, joten pilotointi päätettiin onnistuneesti. Pilotointi suoritettiin 2.11.2022.

3.3.5 Tutkimuksen toteutus

Systemaattinen kirjallisuuskartoitus toteutettiin pilotoinnissa hyväksi todetun protokollan mukaisesti. Aluksi suoritettiin haku Scopus tietokantaan aiemmin määritellyllä hakulausekkeella, jonka jälkeen saadut tulokset suodatettiin aluksi abstraktin ja otsikon perusteella, ja sitten koko tekstin perusteella, jolloin jäljelle jäi hyväksytyt artikkelit. Tutkimuksen toteutus on esitetty kuviossa 9.



Kuvio 9: Hakuprosessin toteutus

Kartoitus suoritettiin seuraavalla hakulausekkeella 5.11.2022:

Hakulauseke
“decentralized identity” OR “self-sovereign identity” OR “distributed identity”

Hausta tuli osumia 408 kappaletta, joista jäi päällekkäisten artikkelien poistamisen jälkeen 405 kappaletta. Koko osumajoukolle tehtiin tämän jälkeen ensimmäinen seulonta lukemalla artikkeleista vain otsikot ja abstraktit. Tässä vaiheessa hylättiin pois artikkelit, joissa jokin hylkäämiskriteereistä täyttyi. Ensimmäisen seulonnan jälkeen artikkeleita jäi jäljelle 157, joille suoritettiin tarkempi seulonta koko tekstin perusteella. Koko tekstin seulonnan jälkeen lopulliseksi määräksi jäi jäljelle 75 artikkelia.

3.3.6 Kartoituksen validointi

Kartoituksen luotettavuuden varmistamista eli validointia suoritettiin jatkuvasti prosessin aikana. Käytännössä tämä ilmentyi valintakriteerien tarkentamisena ja yhteisymmärryksen luomisena tutkijoiden välillä aina epäselvän tilanteen sattuessa. Kun toiselle tutkijoista tuli vastaan artikkeli, jonka valitsemisesta tai hylkäämisestä hän ei ollut täysin varma, keskusteltiin ja tehtiin päätös tämän artikkelin valinnasta yhdessä. Valintakriteereitä tarkennettiin myös tarvittaessa. Suurempien kokonaisuuksien, kuten pilotoinnin, jälkeen käytiin pohdin-

taa yhdessä esiin nousseista huomioista ja varmistettiin, että artikkelien suodattamisessa noudatettiin samoja kriteerejä. Mikäli samoja artikkeleita käytiin useampaan otteeseen läpi, pyrittiin näitä sekoittamaan niin, ettei sama henkilö käynyt yhtä artikkelia läpi useampaan kertaan. Näillä keinoilla kartoituksesta pyrittiin saamaan mahdollisimman luotettava.

3.3.7 Aineiston analysointi

Systemaattisen kirjallisuuskartoituksen aineisto kerättiin Google Sheets -dokumenttiin, johon kirjattiin myös analyysin tulokset. Jos artikkeli päätettiin sisällyttää kartoitukseen koko tekstin perusteella tehtävässä seulontavaiheessa, kerättiin siitä samalla myös tarvittava data kartoitusta varten. Itsehallittavan identiteetin määritelmään liittyen tallennettiin dokumenttiin myös määritelmässä käytetyt viittaukset muihin artikkeleihin. Näin saatiin selville suosituimmat artikkelit SSI:n määritelmään liittyen.

Tämän lisäksi määritelmän kannalta olennaista oli selvittää itsehallittavan identiteetin keskeisimmät komponentit. Dokumenttiin kerättiin tietoa, mitkä komponentit artikkeleissa esiteltiin osana itsehallittavaa identiteettiä. Jokainen esiintynyt komponentti oli taulukossa omana sarakkeenaan ja sai arvon 0 tai 1 sen mukaan esitettiinkö komponentti artikkelissa osana SSI:tä vai ei. Mikäli esitetylle komponentille ei vielä ollut saraketta, lisättiin uusi sarake. Kartoitusta tehdessä merkattiin ylös, minkä artikkelin kohdalla viimeisin komponentti oli lisätty taulukkoon. Kun kaikki artikkelit oli käyty läpi, käytiin ne vielä uudestaan läpi siihen pisteeseen asti, jolloin viimeisin komponentti oli lisätty. Tällä pyrittiin varmistumaan siitä, että jokainen artikkeli tarkasteltiin jokaisen komponentin osalta.

Hyötyjen ja haasteiden suhteen käytettiin samantapaista lähestymistapaa kuin komponenttien tarkastelemisessa. Hyödyt ja haasteet kerättiin kumpikin omiin sarakkeisiinsa. Uuden hyödyn tai haasteen esiintyessä, se lisättiin listalle uutena numeraalisena vaihtoehtona. Näin jokaisen artikkelin kohdalla voitiin sarakkeisiin merkitä numerolistana, mitä hyötyjä ja haasteita artikkelissa oli esitelty. Jos jotkin hyödyt tai haasteet vaikuttivat myöhemmin olevan hyvin päällekkäisiä, saatettiin näitä yhdistää. Hyötyjen ja haasteiden kuvaukset myös muovautuivat pikkuhiljaa tarkemmiksi ja paremmiksi, jonka takia artikkelit käytiin lopuksi vielä läpi ja tarkistettiin, pitikö merkityt hyödyt ja haasteet vielä paikkansa.

Datankeruuvaiheen päätyttyä hyötyjä tuli yhteensä 34 kappaletta ja haasteita vastaavasti 40 kappaletta. Koska määrät olivat niin suuria, nähtiin kerätyt hyödyt ja haasteet tarpeelliseksi kategorisoida. Kategorisointi tapahtui siten, että ensimmäiselle hyödylle listassa nimettiin yhdessä sopiva yläkategoria. Sen jälkeen siirryttiin seuraavaan hyötyyn. Jos tämä nähtiin menevän johonkin olemassa olevaan yläkategoriaan, lisättiin se siihen. Jos ei, nimettiin sille oma yläkategoria. Tätä jatkettiin loppuun saakka, jonka jälkeen kategorioita tarkasteltiin ja tarvittaessa yhdisteltiin keskenään. Kun kategorioita ei enää nähty mahdollisiksi/tarpeellisiksi yhdistää, kategorisointi päätettiin. Sama prosessi toistettiin haasteille. Tämän seurauksena hyödyt saatiin jaettua viiteen (5) kategoriaan ja haasteet kahdeksaan (8).

3.4 Kyselytutkimus

Tässä luvussa käsitellään kyselytutkimusta. Aluksi esitellään Suomen uuden digitaalisen henkilöllisyystodistuksen hanke, johon tutkimuksen kysely pohjautuu. Tämän jälkeen esitellään tutkimuksen toteutus, jossa avataan kyselyn rakennetta ja sen tuottamiseen käytettyjä työkaluja. Lopuksi tarkastellaan tulosten analysointia siinä käytettyjen tilastollisten menetelmien ja työkalujen kautta.

3.4.1 Suomen digitaalinen henkilöllisyystodistus

Suomen Digi- ja väestövirasto (2023) on tätä kirjoitelmaa kirjoittaessa toteuttamassa yhdessä poliisin sekä valtiovarainministeriön kanssa hanketta uudesta digitaalisesta henkilöllisyystodistuksesta. Digitaalisen henkilöllisyystodistuksen toiminta pohjautuu itsehallittavaan identiteettiin ja se on siten yksi käytännön esimerkki SSI:n toteutuksesta. Kehitystyön tuloksena valmistuu mobiilisovellus (Suomi.fi-lompakko). Tämä tulee perinteisen passin ja henkilökortin rinnalle henkilöllisyyden osoittamiseen käynti- sekä verkkoasioinnissa julkisten ja yksityisten toimijoiden palveluissa. Tämän lisäksi hankkeessa kehitetään tunnuslukulaite, jota voi käyttää mobiililaitteen sijaan, mikäli ei itse omista mobiililaitetta. Myös ulkomaalaiset, kuten pakolaiset, voivat hyödyntää tätä uutta henkilöllisyystodistusta henkilöllisyyden osoittamiseen sähköisessä asioinnissa.

Kuten useimmissa muissakin SSI:n käytännön ratkaisuissa, Suomen uuden henkilöllisyystodistuksen käyttö perustuu lohkoketjuteknologiaan. Sen tarkka teknologinen toteutus ei kuitenkaan ole julkista tietoa. Uuden henkilöllisyystodistuksen avulla käyttäjän pitää jakaa vain tarvittava minimimäärä tietojaan, jotta identiteettitietojen tarkistus saadaan suoritettua. Esimerkiksi täysi-ikäisyyttä kysyttäessä käyttäjän on mahdollista näyttää vain olevansa täysi-ikäinen ilman muita tietoja, kuten syntymävuotta. Hankkeen myötä käyttäjällä on myös suurempi kontrolli omien tietojensa hallintaan ja käyttöön. Käyttäjien on myös annettava hyväksyntä, ennen kuin heidän tietojansa voidaan jakaa ja käyttää. Lisäksi digitaalinen henkilöllisyystodistus on toteutettu niin, että sen käyttö, hallinta sekä päivittäminen on läpinäkyvää. Identiteetit säilyvät myös pitkäaikaisesti. Digitaalinen henkilöllisyystodistus on tarkoituksena mukautua yhteiskunnan tarpeisiin ja soveltua uusille digitaalisille alustoille sitä mukaa, kun ne kehittyvät. Sen on myös tarkoitus tulee olemaan myös yhteensopiva Suomen muiden järjestelmien kanssa sekä on Digi- ja väestöviraston mukaan turvallinen ja ylipäänsä hyvää tietoturvaa toteuttava.

Digitaalisen henkilöllisyyden uudistus ei kuitenkaan täytä täysin kaikkia SSI:n toimintaperiaatteita. Vähintään osa käyttäjätiedoista on tallennettu keskitetysti Suomen valtion tietokantoihin. Identiteetti ja siihen liittyvät tiedot eivät samasta syystä ole myöskään siirrettävissä toiseen identiteettipalveluntarjoajaan. Lisäksi todennettavia valtuustietoja ei vielä ole, ainakaan laajamittaisesti, hyödynnetty toteutuksessa. Digitaalisella henkilöllisyystodistuksella ei tästä syystä voi vielä todentaa olevansa opiskelija tai auton ajamiseen valtuutettu, sillä siihen ei voida vielä yhdistää opiskelija- tai ajokortin valtuuksia.

3.4.2 Tutkimuksen toteutus

Kysely on esitetty kokonaisuudessaan liitteessä A. Lomake laadittiin Webropol- kyselysovellusta hyödyntäen. Kyselyn tavoitteena oli selvittää loppukäyttäjien asenteita ja näkemyksiä Suomen digiuudistukseen liittyen. Kysymyksien muodostamisessa käytettiin pohjana kirjallisuuskartoituksen tuloksia. Kyselylomaketta pilotoitiin ensin pienelle vastaajakunnalle, jonka seurauksena kysymyksiä päivitettiin ja kyselyä muotoiltiin uudelleen. Pilotoinnin seurauksena todettiin, että kysely on toimiva ja valmis jaettavaksi.

Kysely koostui viidestä osiosta. Ensimmäinen osio oli saateteksti, joka tuli näkyviin heti, kun kysely avattiin. Saatetekstissä esiteltiin kyselyn sisältö muutamalla lauseella ja kerrottiin kyselyn ja tutkimuksen toteutuksen tavoitteista ja motivaatiosta. Lisäksi saatetekstissä esiteltiin tutkijoiden nimet ja yhteystiedot sekä viitattiin tietosuojailmoitukseen, jossa kerrottiin muun muassa, mitä tietoja käyttäjästä kerätään sekä miten dataa käsitellään ja tallennetaan. Toinen osio oli aihepiirin esittely, jossa esiteltiin kyselyssä tarvittavat olennaiset tiedot sekä käsitteet. Siinä esiteltiin lyhyesti identiteetti, digitaalinen identiteetti, itsehallittava identiteetti sekä Suomen uuden digitaalisen henkilöllisyystodistuksen hanke. Aihepiirin esittely oli myös kiinnitetty osioiden neljä ja viisi alkuun, jotta vastaajan ei tarvitsisi palata takaisin kyselyssä, mikäli he halusivat palata tähän. Seuraavana kyselyssä oli osio vastaajan taustatiedoista. Näitä olivat ikä, koulutus, pääasiallinen toimi, työala, IT-taidot, aiempi tietämys itsehallittavasta identiteetistä sekä halukkuus käyttää Suomen uutta digiuudistusta.

Neljäs ja viides osio liittyivät vastaajien koettuihin hyötyihin ja haasteisiin itsehallittavaan identiteettiin liittyen. Molempien osioiden ensimmäisessä kysymyksessä esiteltiin väittämiä, joiden vastausvaihtoehdot muodostuivat standardisoidun Likert-asteikon vastausvaihtoehdoista. Vastaajan tuli siis valita parhaiten hänen mielipidettään kuvaava vaihtoehto seuraavista viidestä vaihtoehdosta:

- Täysin samaa mieltä (1)
- Samaa mieltä (2)
- En samaa enkä eri mieltä (3)
- Eri mieltä (4)
- Täysin eri mieltä (5)

Neljännessä osiossa esiteltiin ensin väittämiä liittyen digitaalisen henkilöllisyystodistuksen mahdollisiin hyötyihin. Väittämiin tuli valita yksi viidestä vaihtoehdoista, joka kuvaa parhaiten vastaajan mielipidettä väittämästä. Seuraavaksi vastaajien tuli valita kolme heidän mielestään tärkeintä hyötyä edellisessä kysymyksessä esitettyjen väittämien listasta. Viides osio liittyi koettuihin haasteisiin. Tämän rakenne oli sama kuin hyödyissä. Molempien osioiden lopussa oli myös avoin vastauskenttä mahdollisille jatkoajatuksille kysymyksiin liittyen. Avoimet vastauskentät lisättiin kyselyyn, sillä nähtiin, että laadulliset vastaukset tukisivat kyselyn määrällisen puolen tuloksia.

Kysely jaettiin tutkijoiden omissa sosiaalisissa medioissa, kuten Instagramissa ja LinkedInissä. Tämän lisäksi kysely jaettiin myös Jyväskylän yliopiston sähköpostilistoilla. Sosiaalisiin medioihin ja sähköpostilistoille kirjoitettiin kaikkiin lyhyt saateteksti kyselyn jakelun yhteydessä. Kyselyn kohderyhmänä oli kaikki Suomessa asuvat ihmiset. Lisäksi vastaajien tuli käytännössä osata suomea, sillä kysely toteutettiin suomeksi. Kyselyn vastaamisesta ei annettu minkäänlaisia palkkioita, sillä tämä olisi voinut vaikuttaa kyselytuloksien validiteettiin.

3.4.3 Tulosten analysointi

Tulosten analysoimiseen käytettiin apuna Webropolin raportointiosiota sekä Excel ja SPSS-työkaluja. Lisäksi tuloksista luotiin erilaisia taulukoita ja kuvioita tulkinnan helpottamiseksi. Aluksi kaikkia kyselyn eri osa-alueita analysoitiin yleisesti. Tässä hyödynnettiin taulukoita ja kuvioita sekä yleisiä tilastollisia tunnuslukuja, kuten keskiarvoja ja -hajontaa. Tätä analyysiä suoritettiin tausta- ja esitiedoille sekä hyödyille ja haasteille.

Vastauksia analysoidessa huomattiin, että koettujen hyötyjen sekä haasteiden kysymysten vastausvaihtoehdot oli muodostettu normaalista tavasta poikkeavasti – “Täysin samaa mieltä” -vaihtoehto vastaten arvoa 1 ja “Täysin eri mieltä” vastaten arvoa 5. Tulosten tulkinnan helpottamiseksi näiden kysymysten tulokset skaalattiin käänteiseen muotoon:

- Täysin samaa mieltä (5)
- Samaa mieltä (4)
- En samaa enkä eri mieltä (3)
- Eri mieltä (2)
- Täysin eri mieltä (1)

Avointen kysymysten tuloksia analysoitiin siten, että vastaukset kerättiin yhteen, luettiin läpi ja poistettiin niistä sellaiset, jotka eivät vastanneet kysymyksiin lainkaan. Tämän jälkeen vastauksista etsittiin keskenäisiä yhteneväisyyksiä. Avoimista vastauksista etsittiin myös sellaisia huolia tai hyötyjä, joita ei oltu vielä löydetty kartoituksessa tai esitelty kyselyn muissa osioissa.

Saaduille tuloksille hyödyistä ja haasteista toteutettiin myös eksploratiivinen faktorianalyysi. Tämän menetelmän tarkoituksena on löytää muuttujien välisiä yhteyksiä, joiden perusteella muuttujat voidaan ryhmitellä eri faktoreihin. (Metsämuuronen 2011, s. 667). Tuloksia pyrittiin tulkitsemaan myös hyödyntäen klusterianalyysiä sekä ristiintaulukointia. Näiden menetelmien tavoitteena oli verrata hyötyjä ja haasteita eri demografiaryhmittäin. Kyseiset analyysit eivät kuitenkaan tarjonneet tilastollisesti merkittäviä tai tulkittavuudeltaan mielekkäitä tuloksia. Tästä syystä näiden kahden menetelmän tuloksia ei hyödynnetty tutkimuksessa eikä niitä olla esitelty tutkielmassa.

3.4.4 Kyselyn validiteetti

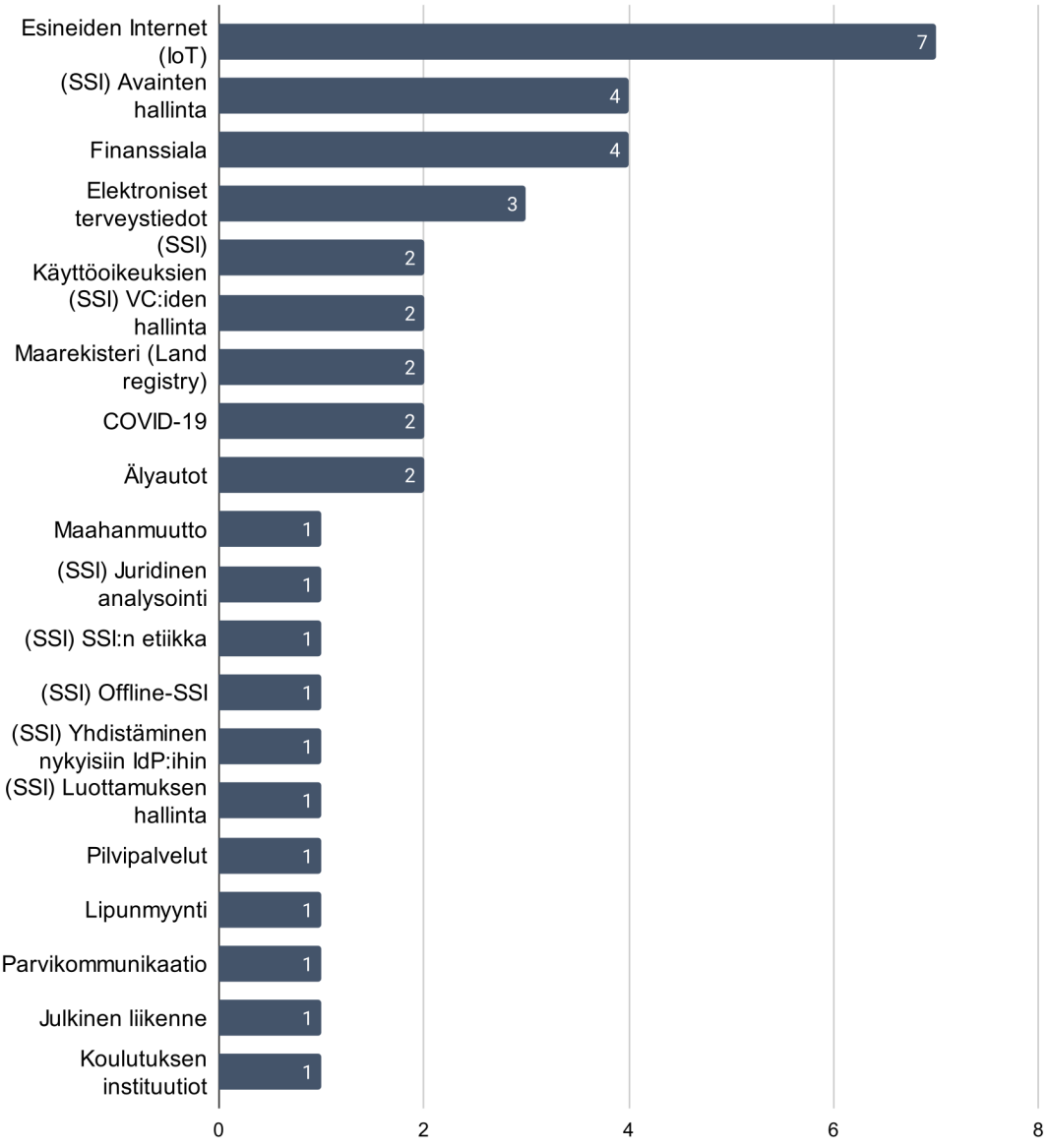
Koska vastaamisesta ei annettu mitään palkkiota, voidaan olettaa, että kaikki kyselyn vastaajat ovat vastanneet kyselyyn omasta tahdostaan ja esittävät siten myös aidosti omia näkemyksiään. Kyselyä sekä sen kysymyksiä muovattiin useaan otteeseen ja sille tehtiin pilotointi ennen lopullista julkaisua. Näin kyselystä saatiin mahdollisimman yksinkertainen ja helposti ymmärrettävä, jotta vastaajat pystyivät vastaamaan kysymyksiin mahdollisimman hyvin. Kyselyn väittämien järjestystä ei kuitenkaan satunnaistettu. Tästä syystä, kysymysten ensimmäisiin väittämiin saatettiin vastata enemmän, kuin viimeisiin väittämiin vain siksi, että ne luettiin ensin. Väittämien järjestyksen satunnaistaminen olisi korjannut tämän vinouman.

4 Kirjallisuuskartoituksen tulokset

Tässä luvussa esitellään kirjallisuuskartoituksen tulokset. Aluksi esitellään tutkimuskohteet, joihin kirjallisuuskartoituksen artikkelit jakautuivat. Tämän jälkeen puhutaan SSI:n määritelmästä kartoituksessa esiin nousseiden viitatuimpien artikkelien kautta. Lopuksi esitellään keskeisimmät komponentit, sekä potentiaaliset hyödyt ja haasteet. Määritelmä ja komponentit on avattu jo kirjoitelman teoria -osiossa, joten tässä luvussa keskitytään vain saatuihin tuloksiin.

4.1 Tutkimuskohde

Kartoituksessa kerättiin tietoa artikkelien tutkimuskohteesta eli alasta tai kontekstista, jota artikkeli tutki tai johon tutkimus oli liitoksissa. Tutkimuskohteet jakautuivat kahteen tyyppiin: SSI:n itsensä tai jonkin sen osa-alueen tutkimiseen sekä SSI:n soveltamiseen johonkin toiseen alaan, kuten esimerkiksi esineiden internetiin. SSI:hin itseensä keskittyvät artikkelit jaoteltiin edelleen alakategorioihin, mikäli tämä oli mahdollista. Suurin osa artikkeleista (36kpl) jäi kuitenkin ilman alakategoriaa, jolloin ne merkattiin yleisellä “SSI itsessään” -kategorialla. Tutkimuskohteet on esitelty kuviossa 10. Yleinen “SSI itsessään” -kategoria jätettiin ulos kuviosta tulkittavuuden säilymiseksi. Kuviota tarkastellessa on siis olennaista huomioida, että siitä puuttuu selvästi suurimman osan kattava yleinen kategoria. SSI:n alakategoriat merkattiin kuvioon etuliitteellä (SSI).



Kuvio 10: Tutkimuskohteet ja niiden määrät

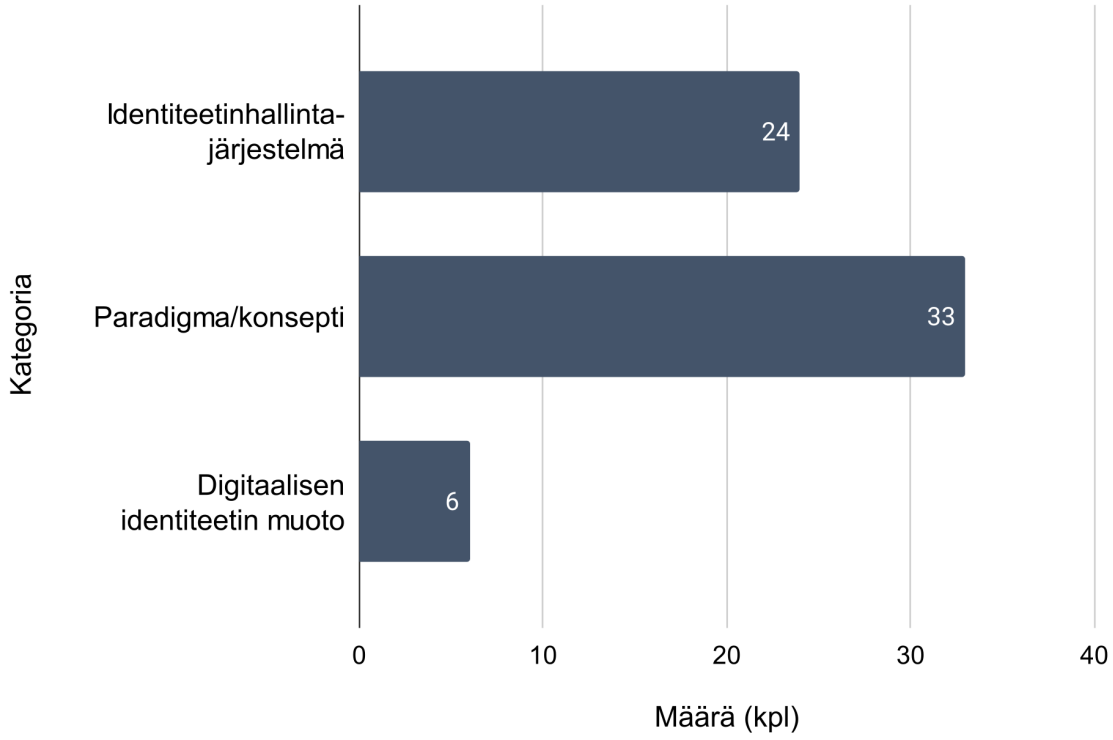
Toinen olennainen huomioitava asia tutkimuskohteiden jakautumisen tuloksia tarkastellessa on, että katsauksen valintakriteerit jättivät ulos paljon tutkimuksia, joiden keskipisteenä oli SSI:n soveltaminen johonkin toiseen alaan. Tähän syynä on se, ettei näiden tutkimusten keskipisteenä ollut SSI itse, jonka takia niiden määritelmä SSI:stä oli useasti suppea eikä niissä esitelty SSI:hin liittyviä potentiaalisia hyötyjä eikä haasteita. Mikäli katsaukseen olisi

otettu mukaan kaikki SSI:tä jollain tavalla käsittelevät artikkelit, esiintyisi näitä tutkimuskohteita todennäköisesti enemmän.

4.2 SSI:n määritelmä ja keskeisimmät komponentit

SSI:n määritelmän selvittämiseksi kartoituksessa kerättiin suoria lainauksia artikkeleissa esiintyvistä SSI:n määritelmistä sekä näissä määritelmissä käytettyjä viittauksia muihin artikkeleihin. Tämän lisäksi artikkeleista kerättiin tietoa siitä, mistä komponenteista SSI koostuu.

Analysoidessa tuloksia määritelmistä kävi ilmi, ettei SSI:n määritelmälle ole vielä selvää konsensusta. Määritelmistä ja niiden eroavaisuuksista johdettiin kolme eri kategoriaa: SSI identiteetinhallintajärjestelmänä, SSI paradigmana tai konseptina ja SSI digitaalisena identiteetin muotona, ks. Kuvio 11. Kaikissa kategorioissa esiintyi myös yhteisiä piirteitä, joita olivat erityisesti käyttäjän täysi hallinta omista identiteettitiedoistaan sekä kolmannen osapuolen hallinnoijan poistuminen tietojen hallinnasta.



Kuvio 11: SSI:n määritelmän kolme kategoriaa sekä artikkeleissa esiintyvien määritelmien jaottuminen näihin kategorioihin määrittäin

Identiteetinhallintajärjestelmänä SSI:tä esiteltiin muun muassa seuraavilla tavoin:

> SSI refers to a new IMS whereby the user should fully own his/her identity data without any intervention from an outside administration. (Dib ja Toumi 2020, s. 21)

> SSI is an identity management system that allows users to fully own and manage their digital identities. (Daniela Pöhn, Michael Grabatin ja Wolfgang Hommel 2021, s. 3)

> The identity management model evolved in the following order: personal identity model, combined identity model, and self-sovereign identity model as the perception of personal information changed. Self-Sovereign Identity (SSI) is not a method in which a company controls personal information, but a met-

> hod in which individuals directly issue and issue personal information. (Kim ym. 2021, s. 2)
>
> This self-sovereign IDM model is an improvement on the federated IDM model, where it removes the third-party IDP and offers a direct connectivity between a user and organisation. (Naik ja Jenkins 2020b, s. 91)

Paradigmana tai konseptina SSI taas esiintyi määritelmissä muun muassa seuraavasti:

> SSI is the concept where organizations and individuals have whole ownership of their identities along with self defined attributes and identifiers. (Pinky Bai ym. 2022, s. 4)
>
> Self-Sovereign Identity (SSI) refers to the digital movement that recognizes that an individual should own and control their digital identity without relying on a third party. (Naghmouchi, Ayed ja Laurent 2022, s. 2)
>
> The paradigm of SSI puts the user at the centre of the identity ecosystem and back in control of his or her identity data. Identities for various subjects can be registered, resolved, updatedor revoked without a central authority. (Richter ja Anke 2021, s. 107)
>
> A new paradigm has gained momentum outside enterprise-internal setups: Self-Sovereign Identity (SSI) is a term describing user-centered, user-administered decentralized approach and role model. (Kuperberg ja Klemens 2022, s. 1)

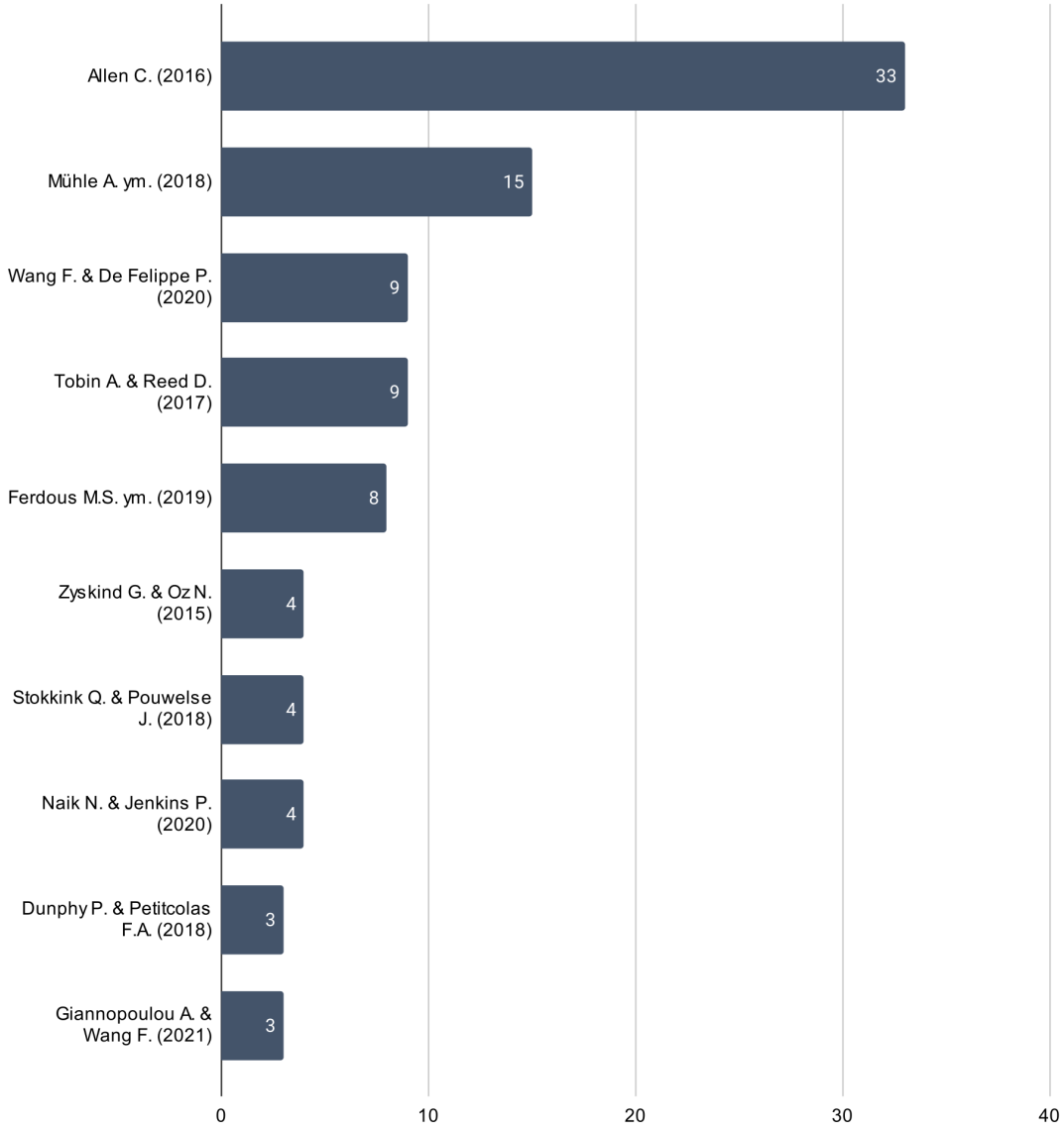
SSI:hin digitaalisen identiteetin muotona laskeutui muun muassa seuraavat määritelmät:

> Self-Sovereign Identity (SSI) is a sovereign, enduring and portable identity for any person, organization, or body, that allows its owner to access all relevant digital services by utilising verifiable credentials linked to the identity in a privacy preserving manner. (Naik ja Jenkins 2020d, s. 1)
>
> A digital representation of the individuals' characteristics, description, and identifiers where no government, or organization, can violate our right to choose our level of privacy or celebrity with our identity attributes. (Satybaldy, Has-

selgren ja Nowostawski 2022, s. 3)

> Considering an identity to be composed of an identifier associated with a set of name-value attributes, the full self-sovereign identity of an individual is the collection of all identities (i.e. identifiers and attributes) that span a range of decentralized domains, such that the individual is in full control of these identities. (Fedrecheski ym. 2020, s. 1)

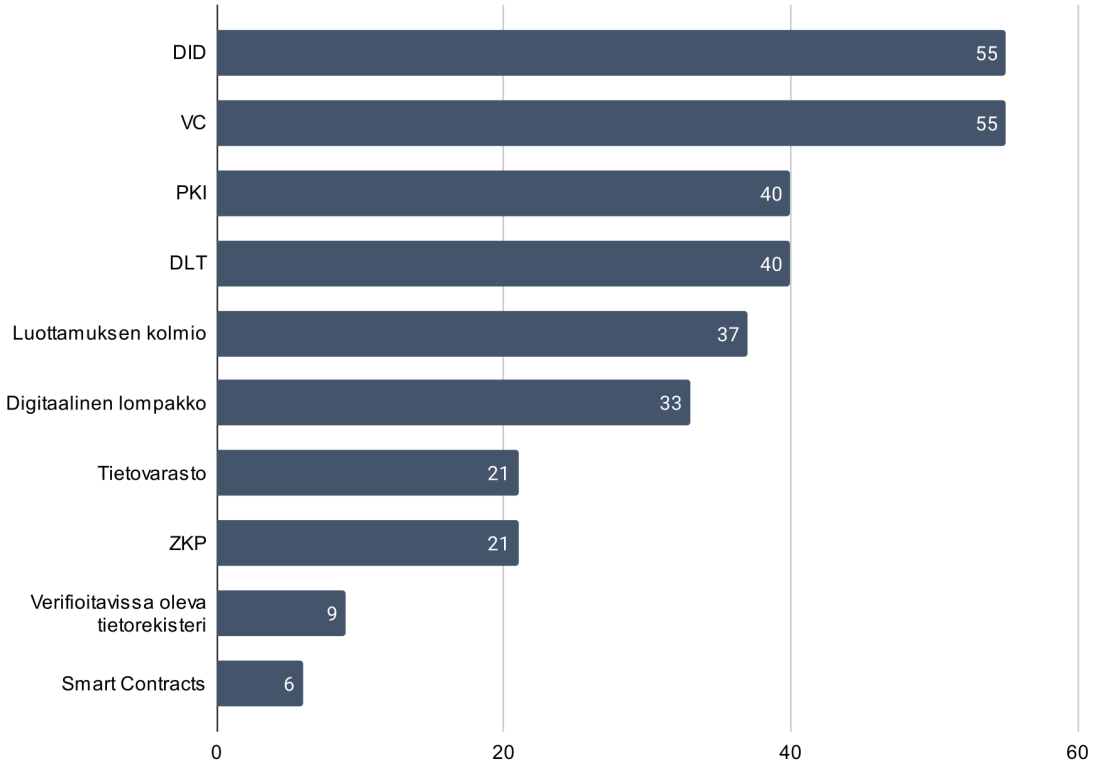
Kuviossa 12 esitellään viitatuimmat artikkelit. Selkeästi eniten artikkeleissa viitattiin Christopher Allenin (2016) "The Path to Self-Sovereign Identity" -blogikirjoitukseen. Allenin blogista keskeisin SSI:n määritelmä on kymmenen ohjenuoraa, jotka on esitelty luvussa 2.2. Toiseksi viitatuin artikkeli oli Mühle ym. (2018) "A survey on essential components of a self-sovereign identity", joka esitteli SSI:n pääkomponentit. Wang ja De Filippi (2020) määrittelivät selkeästi termistöä liittyen itsehallittavaan identiteettiin ja sen komponentteihin. Lisäksi he esittelivät jo olemassa olevia käytännön toteutuksia aiheesta. Tobin ja Reed (2016) kirjoittivat Sovrinin valkoisen kirjan, joka on ensimmäisiä käytännön toteutuksia SSI:stä. Tämä kirja kategorisoi myös Allenin kymmenen ohjenuoraa ja esittää määritelmän itsehallittavalle identiteetille. Ferdous, Chowdhury ja Alassafi (2019) taas esittävät laajan ja kattavan määritelmän SSI:lle ja sen komponenteille helposti luettavassa muodossa. Loput esitellyistä artikkeleista ovat myös suosittuja artikkeleita SSI:n tutkimuksessa.



Kuvio 12: Kartoituksessa valittujen artikkeleiden yleisimmät viittaukset

Kuviossa 13 esitellään SSI:n keskeisimmät komponentit. Komponentit, joihin viitattiin kartoituksessa vain yhdessä tai kahdessa artikkelissa, on jätetty ulos kuviosta. Kaikki esiintyvät komponentit on selitetty luvussa 2.4, minkä takia niitä ei esitellä suuremmin tässä luvussa. DID ja VC ovat selkeästi keskeisimmät komponentit itsehallittavassa identiteetissä. Tämä johtuu todennäköisesti siitä, että ne ovat W3C:n määrittelemiä standardeja. Lisäksi PKI ja DLT nousivat esiin monessa artikkelissa. Nämä ovat keskeisiä komponentteja itse-

hallittavaan identiteettiin liittyen etenkin lohkoketjua hyödynnettäessä. Verifioitavissa oleva tietorekisteri ja älysopimukset nousivat esiin vähiten.



Kuvio 13: SSI:n keskeisimmät komponentit ja niiden esiintymismäärät artikkeleissa

4.3 Potentiaaliset hyödyt

Tässä luvussa esitellään esiin nousseet potentiaaliset hyödyt, joita SSI:n käyttöönotosta voi seurata. Tulokset esitellään taulukossa 3. Hyödyt on jaettu yläkategorioihin. Taulukon “Määrä”-sarake kuvastaa kyseistä hyötyä esittävien artikkelin määrää. Alla esitetyssä taulukossa jokaisesta yläkategoriasta on esitelty vain kolme eniten esiintymää omaavat hyödyt. Kaikki hyödyt määrittäin on esitelty liitteessä C. Yläkategorian rivillä näkyy myös sen kategorian artikkelien yhteenalskettu määrä. Yläkategoriat ovat esiintymisten määrien järjestyksessä seuraavat: yksityisyys (62 kpl), turvallisuus (40 kpl), käytettävyys (32 kpl), resurssien säästäminen (8 kpl) ja sekalainen (8kpl).

Hyöty	Määrä
Yksityisyys (yht.)	62
Käyttäjällä on täysi kontrolli omasta identiteetistään	23
Yksityisyyden turva (privacy)	21
Datan minimalisointi (data minimalization)	6
Muut	12
Turvallisuus (yht.)	40
Tietoturva (data protection/security)	20
Datan pysyvyys (data permanence)	6
Luotettavuus	5
Muut	9
Käytettävyys(yht.)	32
Parantaa yleisesti käyttäjäkokemusta	8
Siirrettävyys (portability)	8
Yhteentoimivuus (interoperability)	5
Muut	11
Resurssien säästäminen (yht.)	8
Resurssien säästäminen/tehokkuus organisaatioille (esim. kulut)	4
Asiakkaan sisäänottoprosessin parantaminen ja tehostaminen	2
Työnkulun automatisointi (automated workflow)	1
Prosessien yksinkertaistaminen	1
Sekalainen (yht.)	8
Saatavuus	4
Käyttö ei vaadi paljoa suorituskykyä/muistia (IoT)	1
Käyttäjillä mahdollista saada palkkio datan jakamisesta	1
Muut	2

Taulukko 3: Potentiaaliset hyödyt kategorioittain suurimmasta pienimpään

Yksityisyyden kategoriasta keskeisimpinä hyötyinä nousivat käyttäjän täysi kontrolli omasta identiteetistä (23 kpl) sekä parempi yksityisyyden turva (21 kpl). Muita esiin nousseita

hyötyjä olivat datan keräämisen minimalisointi (6 kpl), keskitetyn hallinnon eliminointi (6 kpl) sekä läpinäkyvyys kerättävästä datasta (5 kpl). Oikeus tulla unohdetuksi eli käyttäjän mahdollisuus poistaa omat tietonsa esiintyi yhden kerran.

Turvallisuudesta keskeisin esiin noussut hyöty oli parempi tietoturva (20 kpl). Muita useammin esiin nousseita hyötyjä olivat datan pysyvyys (6 kpl), luotettavuus (5 kpl) ja yhden virhepisteen eliminointi (engl. single point-of-failure) (4 kpl). Vähemmän esiintyneitä hyötyjä olivat parempi petosten havaitseminen (2 kpl), datan muuttumattomuus (2 kpl) ja valvonnan väheneminen (1 kpl).

Käytettävyydessä ei noussut yhtään selkeästi muita enemmän esiintyvää hyötyä. Eniten mainittuja hyötyjä olivat yleisesti parempi käyttäjäkokemus (8 kpl) ja siirrettävyys eli esimerkiksi mahdollisuus vaihtaa digitaalisen lompakon tarjoajaa halutessaan (8 kpl). Useammin kuin kerran esiintyneitä hyötyjä olivat automaattinen auktorisointi (3 kpl), ajan säästyminen (3 kpl) sekä automaattinen autentikointi (2 kpl). Kerran esiintyneitä hyötyjä olivat tunnusten hallinnan helpottuminen, fyysisen identiteettitodistuksen kantamisen tarpeen poistuminen sekä vanhojen ongelmallisten toimintamallien parantaminen tai poistuminen.

Resurssien säästämisestä ei myöskään ollut selkeästi muita enempää esiintyviä hyötyjä. Esitettyjä hyötyjä olivat resurssien säästäminen ja parempi tehokkuus organisaatiolle (4 kpl), asiakkaan sisäänottoprosessin tehostaminen ja kehittäminen (2 kpl), työnkulun automatisointi (1 kpl) sekä prosessien yksinkertaistaminen (1 kpl).

Sekalainen-kategoriaan menivät ne hyödyt, joita ei saatu sijoitettua muihin kategorioihin, ja joista ei saatu muodostettua enää uutta yläkategoriaa. Näistä eniten esiintyvä hyöty oli saatavuus (4 kpl). Loput sekalaisista hyödyistä mainittiin kerran. Näitä olivat laitteiston suorituskyvyn vaatimusten keventyminen (1 kpl), käyttäjille mahdollisten palkkioiden tarjoaminen oman datan jakamisesta (1 kpl), olemassa olevat standardit (1 kpl) sekä COVID-tartujen mahdollinen hidastaminen (1 kpl).

4.4 Potentiaaliset haasteet

Tässä luvussa esitellään esiin nousseet SSI:hin liittyvät potentiaaliset haasteet. Tulokset esitellään taulukossa 4. Hyötyjen tapaan haasteet on jaoteltu yläkategorioihin ja taulukon "Määrä"-sarake vastaa kyseisen haasteen esittävien artikkelin määrää. Alla esitetyssä taulukossa jokaisesta yläkategoriasta on esitelty vain eniten esiintymiä omaava haaste. Kaikki haasteet määrittäin on esitelty liitteessä D. Haasteiden yläkategoriat ovat seuraavat: tekniset haasteet (33 kpl), kehityksen ja standardien puute (29 kpl), turvallisuuden ja yksityisyyden haasteet (18 kpl), luottamuksen haasteet (17 kpl), sekalaiset haasteet (15 kpl), kulujen nousu (13 kpl), käytettävyyden haasteet (9 kpl) sekä muutosvastahakoisuus (8 kpl).

Haaste	Määrä
Tekniset haasteet (yht.)	33
Tunnusten (avaimen) palautus	18
Muut	15
Kehityksen ja standardien puute (yht.)	29
Standardien ja yhteisymmärryksen puute	14
Muut	15
Turvallisuuden ja yksityisyyden haasteet (yht.)	18
Digitaalisen lompakon joutuminen vääriin käsiin	5
Muut	13
Luottamuksen haasteet (yht.)	17
“Luottamusankkurin” puute	11
Muut	6
Sekalaiset haasteet (yht.)	15
Lailliset haasteet (esim. GDPR, eIDAS)	7
Muut	8
Kulujen nousu (yht.)	13
Vaatii suuria muutoksia organisaatioissa ja infrastruktuureissa	10
Muut	2
Käytettävyyden haasteet (yht.)	9
Käyttäjäystävällisyys	6
Muut	3
Muutosvastahakoisuus (yht.)	8
Vastahakoisuus muutoksille	4
Muut	4

Taulukko 4: Potentiaaliset haasteet kategorioittain suurimmasta pienimpään

Teknisistä haasteista selvästi esiintynein haaste oli tunnusten eli avainten palautus niiden hävitessä (18 kpl). Muita enemmän kuin kerran esiintyneitä haasteita oli skaalautuvuuden heikkous (4 kpl), varastoinnin rajoitteet (3 kpl) ja Internetin tai muiden SSI:n käytölle tar-

vittavien laitteiden puuttuminen joillakin käyttäjäryhmillä (2 kpl). Kerran esiin nousseita haasteita olivat pitkä transaktioiden validointiaika, “ID Squatting” eli liiallisen ID:iden rekisteröimisen rajoittamisen vaikeus, mahdottomuus toteuttaa SSI:tä ilman lohkoketjua, offline-käytön vaikeus, spesifien toiminnallisuuksien vaatimukset IoT:n kontekstissa sekä nykyisten lohkoketjujen toteutusten sopimattomuus SSI:n toteuttamiseen. Useat näistä, kuten skaalautuvuus, varastoinnin rajoitteet ja transaktioiden validointiaika, ovat lohkoketjuteknologiaan liittyviä haasteita.

Kehityksen ja standardien puute -kategoriassa eniten esiintyvä haaste oli standardien ja yhteisymmärryksen puute (14 kpl). Muita haasteita olivat SSI:n kehityksen ja tutkimuksen puute (7 kpl), teknologiaosaamisen puute (4 kpl), SSI:n laajamittaisen käytön puute (3 kpl) sekä SSI:n attribuuttien yhteensopivuus kaikkien maiden välillä puhuttaessa globaalista SSI-toteutuksesta (1 kpl).

Turvallisuuden ja yksityisyyden haasteissa ei esiintynyt yhtä haastetta selvästi enempää kuin muita. Enemmän kuin kerran esiintyneitä haasteita olivat riski digitaalisen lompakon eli identiteetin joutumisesta väärin käsiin (5 kpl), suljettuun DLT:hen (3 kpl) ja vastaavasti avoimeen DLT:hen (2 kpl) liittyvät ongelmat SSI:n toteutustavan mukaan sekä vastuuvelvollisuuden määrittäminen ilman tapahtumien tallentamista julkisesti (3 kpl). Kerran esiintyneitä haasteita olivat Sybil-hyökkäykset, uuden avaimen luominen aiemman yksityisen avaimen pohjalta nousevat ongelmat (“Key rotation” -ongelma), alttisu DDoS-hyökkäyksille, mahdollisuus omien tunnusten myymiselle jakamiselle sekä jäljitettävyys.

Luottamus-kategoriassa eniten esiintynyt haaste oli “Luottamusankkurin” puute (11 kpl). Koko kategoria koostui suurimmilta osin tästä haasteesta. Luottamusankkurilla (engl. Trust anchor) viitataan tahoon, johon kaikki voivat luottaa esimerkiksi todennettaessa jonkin osapuolen oikeellisuutta. Koska, SSI:ssä ei ole kolmansia osapuolia, ei luottamusankkuriakaan siis löydy. Lisäksi tässä kategoriassa esiintyi datan eheys (3 kpl), luottamuksen puute hallitusta kohtaan (2 kpl) sekä vaikeus saavuttaa korkean tason LoA (Level of Assurance) (1 kpl).

Sekalaiset-kategoriassa meneteltiin samalla lailla, kuin hyödyt-osiossakin. Sinne menivät ne haasteet, joita ei saatu sijoitettua muihin kategorioihin, ja joista ei saatu muodostettua

uutta yläkategoriaa. Näistä suurimpina osioina olivat lailliset haasteet (7 kpl) sekä saatavuus ja neutraalisuus (6 kpl). Laillisiin haasteisiin lukeutui ongelmat liittyen esimerkiksi GDPR-asetuksiin. Lailliset haasteet olivatkin jo omana osionaan hieman pirstaloituneet, sillä artikkeleissa saatettiin viitata johonkin spesifiin, mahdollisesti maa- tai aluekohtaiseen lakiin tai säädökseen, tai jonkin tietyn SSI:n sovellutusmuodon spesifiin lailliseen haasteeseen. Saatavuus ja neutraalisuus viittaa siihen, että kaikilla ei välttämättä ole tasapuoliset mahdollisuudet käyttää ja hyödyntää itsehallittavaa identiteettiä, tai joillain ei ole mahdollisuutta käyttää sitä lainkaan. Kolmantena haasteena esiintyi kontrollin lisääntyminen (3 kpl), joka viittaa nimensä mukaan mahdollisuuteen siitä, että kontrollin määrä voi lisääntyä SSI:n käyttöönoton myötä.

Kulujen nousussa eniten esiintynyt haaste oli suurien muutoksien tarve organisaatioissa ja infrastruktuureissa (10 kpl). Muutosten toteutus aiheuttaa monella tapaa kuluja organisaatioille kuin myös yksilöillekin. Tarpeita esiteltiin erilaisia ja ne voivat olla monissa paikoissa perustavanlaatuisia. Esimerkiksi koko digitaalinen infrastruktuuri voidaan joutua joissain määrin rakentamaan uudelleen tai ylipäänsä luomaan, jos sellaista ei vielä ole. Lisäksi kulujen nousussa oli esitelty kehityksen ja ylläpidon kustannukset (2 kpl), joka menee osaltaan päällekkäin ylemmän haasteen kanssa sekä viimeisenä hieman haaste: Lohkoketjujen transaktioiden validoinnin kustannukset (1 kpl).

Käytettävyyden haasteisiin lukeutui kolme haastetta: Käyttäjäystävällisyys (6 kpl), uupumus suostumuksen antamisesta (2 kpl) sekä vaikeus tehdä muutoksia käyttäjän tietoihin (1 kpl). Käyttäjäystävällisyys on jatkuva haaste digimaailmassa, sillä sovellukset voisivat aina olla käyttäjäystävällisempiä. Uupumus suostumuksen antamisesta eli “Consent fatigue” on myös kasvava ongelma regulaatioiden lisääntymisen myötä. Koska käyttäjällä on SSI:n myötä enemmän valtaa, hänen pitää myös itse jakaa enemmän suostumuksia datansa käyttämiseksi. Tämä voi osoittautua työlääksi ja aikaa vieväksi.

Viimeinen kategoria on muutosvastahakoisuus. Tässä kategoriassa eniten esiintynyt haaste on vastahakoisuus muutokselle (4 kpl). Muutosvastarintaa esiintyy kaiken uuden teknologian ja ylipäänsä muutoksen yhteydessä. Tietämys asiasta ja selkeä perehdytys auttavat tähän. Tämän lisäksi kategoriaan kuuluu hallituksen vastaisuus itsehallittavuutta kohtaan (2 kpl) sekä SSI:n todistettavuus kannattavaksi liiketoimeksi (2 kpl). Vastustusta muutokselle

voi siis esiintyä monella eri tasolla käyttäjätasolta hallitukseen saakka. Myös SSI:n todistaminen kannattavaksi liiketoiminnaksi on vaikeaa, sillä siitä ei vielä ole monia konkreettisia käytännön toteutuksia.

5 Kyselytutkimuksen tulokset

Kyselyyn vastasi 226 henkilöä. Seuraavaksi esitellään kyselytutkimuksen tulokset. Vastauksista esitellään ensin tausta- ja esitiedot. Tämän jälkeen käsitellään koettujen hyötyjen sekä haasteiden tulokset omissa kappaleissaan. Lopuksi esitellään ekspolaritiivisesta faktorianalyysistä nousseet tulokset.

5.1 Tausta- ja esitiedot

Taulukossa 5 on esitelty vastaajien demografiatiedot. Niihin kuuluu ikä, koulutus sekä pääasiallinen toimi. Vastaajista suurin osa oli 18-30 vuotiaita, mikä selittyy sillä, että kyselyä jaettiin tutkijoiden sosiaalisten medioiden kautta sekä Jyväskylän yliopiston sähköpostilistalla. Enemmistö sekä tutkijoiden sosiaalisten medioiden kontakteista, että yliopiston opiskelijoista kuuluvat kyseiseen ikäryhmään. Kyselyyn vastanneissa ei ollut lainkaan alle 18-vuotiaita eikä yli 70 vuotiaita, joten vastanneiden ikähaarukka oli 18-70 vuotiaat. Vastanneiden koulutuksessa selkeästi suurimmat vastaajaryhmät olivat alempi -, sekä ylempi korkeakoulututkinto. Vastaajissa oli myös kohtalaisen paljon ylioppilas- tai ammatillisen tutkinnon koulutustasoa ja muutama tohtorikoulutettu. Vastaajista lähes kaikki olivat joko työssäkäyviä tai opiskelijoita. Työssäkäyviä oli kuitenkin selkeästi opiskelijoita enemmän. Loput vastaajista jakautuivat melko tasaisesti jäljelle jääneisiin toimiin (yrittäjä, eläkeläinen, työtön, jokin muu). Vastaajien ikään sekä jakelukanaviin suhteutettuna koulutustason ja pääasiallisen toimen tulokset olivat odotettuja.

Kysymys	Vastaus	kpl	Prosentti
Ikä (vuosina)	Alle 18	0	0%
	18-30	161	71.2%
	31-40	28	12.4%
	41-50	16	7.1%
	51-60	17	7.5%
	61-70	4	1.8%
	71+	0	0%
Koulutus	Peruskoulu	0	0%
	Ylioppilas- tai ammatillinen tutkinto	42	18.6%
	Alempi korkeakoulututkinto	98	43.4%
	Ylempi korkeakoulututkinto	82	36.3%
	Tohtorikoulutus	3	1.3%
	Jokin muu koulutus	1	0.4%
Pääasiallinen toimi	Työssäkäyvä	129	57.1%
	Yrittäjä	4	1.8%
	Opiskelija	82	36.3%
	Eläkeläinen	6	2.6%
	Työtön	2	0.9%
	Jokin muu	3	1.3%

Taulukko 5: Vastaajien ikä, koulutus ja pääasiallinen toimi määrittäin

Kysymyksessä työalasta oli paljon vastausvaihtoehtoja, jonka takia vastaukset tähän kysymykseen jakautuivat laajemmin. Selkeästi eniten vastauksia tuli kuitenkin “En ole töissä” -vaihtoehdolle, sekä “Tietojenkäsittely ja IT” -alalle. Tietojenkäsittely ja IT-alan suuri määrä voi selittyä osaksi sillä, että suuri osa tutkijoiden sosiaalisten medioiden kontakteista työskentelee IT-alalla. Lisäksi kyselyn aihe liittyy tähän aihepiiriin, joten alalla työskentelevät tai opiskelevat saattavat luonnollisesti kiinnostua enemmän aiheesta. Näiden kahden vaihtoehdon lisäksi moni vastaajista työskenteli muun muassa “terveydenhuolto” sekä “liiketoiminta, konsultointi ja johtaminen” -aloilla. Vastaajien työalat on esitelty taulukossa

6.

Ala	kpl	Prosentti
Tietojenkäsittely tai IT	51	23.3%
En ole töissä	50	22.8%
Terveydenhuolto	21	9.6%
Liiketoiminta, konsultointi tai johtaminen	16	7.3%
Julkiset palvelut tai julkishallinto	13	5.9%
Jokin muu	12	5.5%
Koulutusala	12	5.5%
Insinöörityö tai valmistusteollisuus	8	3.6%
Kiinteistöt tai rakentaminen	5	2.3%
Kirjanpito, pankki- tai rahoitusala	5	2.3%
Lääketiede ja lääkevalmisteet	4	1.8%
Vapaa-aika, urheilu tai matkailu	4	1.8%
Kuljetus tai logistiikka	3	1.4%
Markkinointi, mainonta tai PR-toiminta	3	1.4%
Sosiaalihuolto	3	1.4%
Vähittäismyynti	3	1.4%
Rekrytointi tai HR	2	0.9%
Hyväntekeväisyys- tai vapaaehtoistyö	1	0.5%
Oikeus ja laki	1	0.5%
Lainvalvonta ja turvallisuus	1	0.5%
Ympäristö tai maatalous	1	0.5%
Energia- ja yleishyödylliset palvelut	0	0%
Luovat taiteet tai muotoilu	0	0%
Media	0	0%
Tapahtumien tai tilaisuuksien järjestäminen	0	0%

Taulukko 6: Vastaajien työalat määrittäin

Tausta- ja esitiedoissa vastaajista kerättiin myös tietoa liittyen IT-taitoihin, aihepiirin aikai-

sempaan tietämykseen, sekä halukkuudesta digitaalisen henkilöllisyystodistuksen käyttöönotolle. Nämä tiedot on esitetty taulukossa 7. IT-taidoissa suurin osa vastauksista jakautui kohtiin “Pätevä” sekä “Kohtalaisen pätevä”. Suhteellisen moni vastaajista koki myös olevansa erittäin pätevä. Aihepiirin aikaisempaan tietämykseen liittyen, vastaajat eivät tulosten mukaan tienneet itsehallittavasta identiteetistä eikä uudesta henkilöllisyystodistuksesta ennestään kovin paljoa. Suurin osa vastauksista painottui “Vähän”, “En mitään” ja “Hieman” -vaihtoehtoihin. Mainittavaa kuitenkin on, että suuri osa (n. 75 %) vastaajista kuitenkin tiesi jotain aihepiiriin liittyen. Suurin osa vastaajista tulisi todennäköisesti ottamaan uuden digitaalisen henkilöllisyystodistuksen käyttöön. Osa (n. 20 %) ei kuitenkaan osannut sanoa tai ottaa kantaa asiaan. Hyvin pieni osa vastaajista ei todennäköisesti ottaisi uudistusta käyttöön.

Kysymys	Vastaus	kpl	Prosentti
Miten pätevä koet olevasi IT-taidoissa?	Erittäin pätevä	35	15.5%
	Pätevä	94	41.6%
	Kohtalaisen pätevä	77	34.1%
	En erityisen pätevä	19	8.4%
	En lainkaan pätevä	1	0.4%
Miten paljon tiedät ennestään itsehallittavasta identiteetistä tai Suomen uudesta digitaalisesta henkilöllisyystodistuksesta?	Paljon	4	1.8%
	Jonkin verran	31	13.7%
	Hieman	54	23.9%
	Vähän	83	36.7%
	En mitään	54	23.9%
Miten todennäköisesti tulet ottamaan uuden digitaalisen henkilöllisyystodistuksen käyttöön?	Hyvin todennäköisesti	88	38.9%
	Melko todennäköisesti	77	34.1%
	En osaa sanoa	47	20.8%
	Melko epätodennäköisesti	10	4.4%
	Hyvin epätodennäköisesti	4	1.8%

Taulukko 7: Vastaajien IT-taidot, aihepiirin tuntemus ja halukkuus digitaalisen henkilöllisyystodistuksen käyttöönotolle

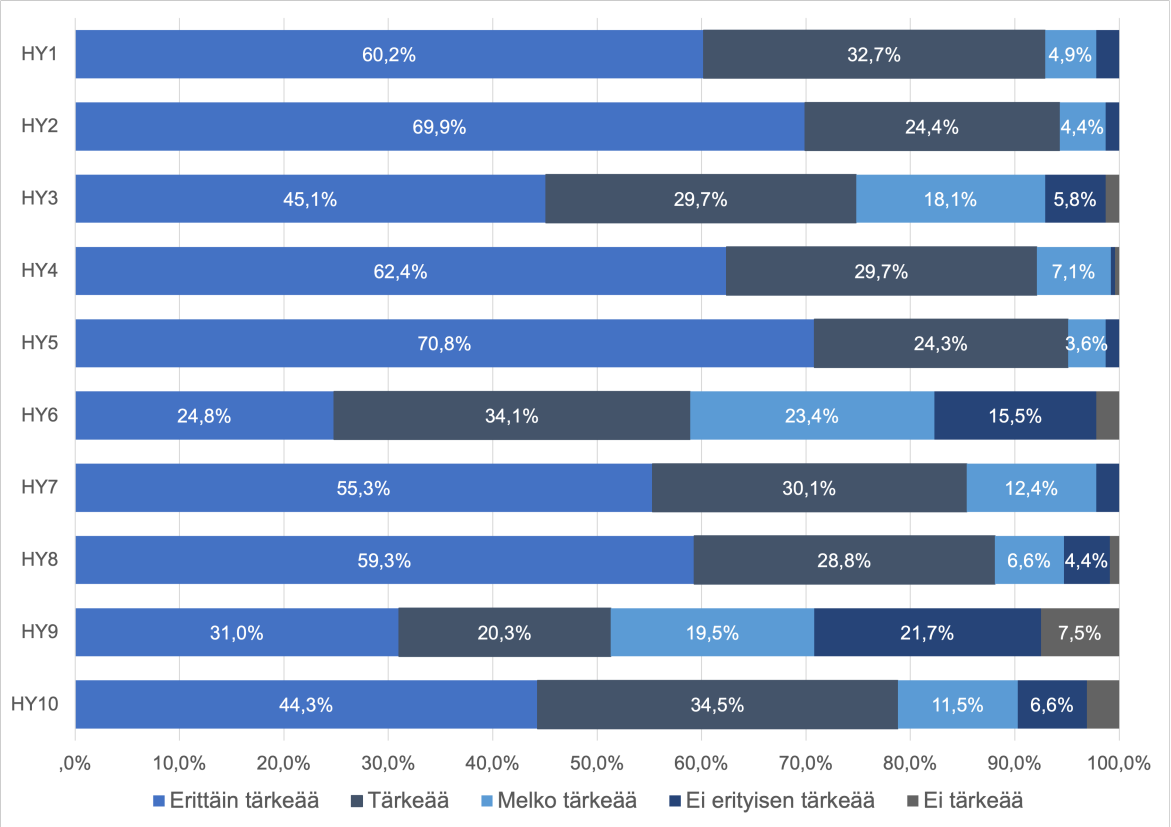
5.2 Koetut hyödyt

Koettujen hyötyjen tulokset kysymykseen 8 on esitetty taulukossa 8. Mitä korkeampi tulosten keskiarvo oli, sitä enemmän samaa mieltä vastaajat olivat olleet esitetyn väitteen kanssa. Koska suurin osa tuloksista oli lähellä maksimiarvoa 5, voidaan todeta vastaajien olleen pitkälti samaa mieltä väittämien kanssa. Vastaajat näkivät siis kaikki koetut hyödyt tärkeinä. Myös mediaani kaikissa väitteissä oli 4 tai 5, mikä vahvistaa tätä edelleen. Suurimmassa osassa väittämiä myös keskihajonta oli alhainen (pääosin alle 1,1). Keskiarvon mukaan vastaajat kokivat hyödyt HY5, HY2, HY4, HY1, HY8 ja HY7 tärkeimmiksi (järjestyksessä tärkeimmästä vähiten tärkeään). Nämä kaikki kuusi hyötyä saavuttivat korkean keskiarvon. Loppujen neljän hyödyn keskiarvot olivat myös suhteellisen korkeat, mutta selkeästi näitä edeltäviä hyötyjä alhaisemmat.

Koodi	Hyöty	Keskiarvo	Mediaani	Keskihajonta
HY1	Minulla on mahdollisuus päättää itse, miten tietojani jaetaan ja käytetään	4.51	5.00	0.69
HY2	Yksityisyyteni on paremmin turvattu	4.63	5.00	0.64
HY3	Minulla on mahdollisuus jakaa vain minimimäärän tietoja itsestäni	4.12	4.00	0.99
HY4	Tietojeni jakaminen ja käyttö on läpinäkyvää	4.53	5.00	0.69
HY5	Henkilötietojeni tietoturva paranee	4.65	5.00	0.62
HY6	Toimintani valvominen vähenee	3.64	4.00	1.08
HY7	Tunnistautuminen on helppoa ja intuitiivista	4.38	5.00	0.79
HY8	Voin käyttää samaa henkilöllisyystodistusta useissa järjestelmissä ja maissa	4.41	5.00	0.87
HY9	Minun ei tarvitse kantaa erillistä fyysistä henkilöllisyystodistusta mukanani	3.46	4.00	1.33
HY10	Kaikilla on mahdollisuus ottaa uusi henkilöllisyystodistus käyttöön	4.10	4.00	1.05

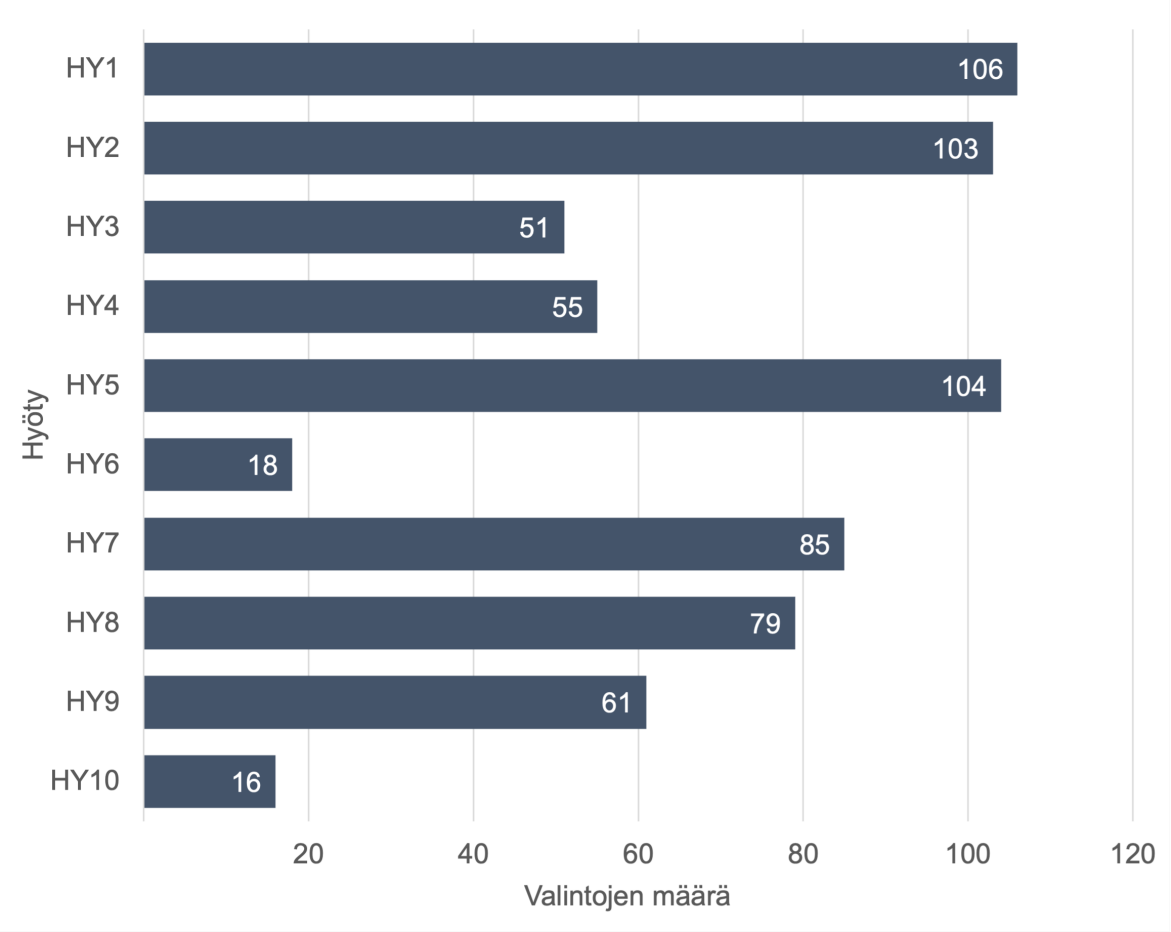
Taulukko 8: Vastaukset kysymykseen 8: “Ilmoita, miten tärkeää seuraavien väittämien toteutuminen on sinulle uuden digitaalisen henkilöllisyystodistuksen osalta”

Kuviossa 14 on esitelty tarkemmin hyötyjen vastauksien jakautumista. Tästä voidaan huomata, että “Ei tärkeää” -vaihtoehtoa on vastattu kokonaisuudessaan hyvin vähän. Myös “Ei erityisen tärkeää” -vaihtoehtoa on vastattu aika pitkälti vain väittämissä HY9 ja HY6. Kuviosta vahvistuu myös, että vaihtoehtoja 5 ja 4, eli “Erittäin tärkeää” ja “Tärkeää” on vastattu selkeästi eniten. Kuvio vahvistaa myös keskihajontaan liittyviä lukuja, eli väittämissä HY9, HY6, HY10 ja HY3 on eniten hajontaa vastausten välillä.



Kuvio 14: Vastaukset kysymykseen 8 – Jakautuminen vastauksittain

Kuvio 15 esittää vastaajien tärkeimmiksi koetut hyödyt. Näiden tulosten mukaan hyödyt HY1, HY5 sekä HY2 nähtiin tärkeimpinä hyötyinä. Selkeästi vähiten tärkeänä nähtiin hyödyt HY6 sekä HY10. Kun kuvioiden 8, 15 ja 14 tuloksia tarkastellaan kokonaisuutena, huomataan, että hyödyt HY1, HY2, HY5, HY7 ja HY8 nähtiin tärkeinä kummassakin osiossa. Hyötyä HY6 ei nähty niin tärkeänä kummassakaan osiossa. Muiden hyötyjen osalta hyötyjen koettu tärkeys vaihteli jonkun verran osioiden tulosten välillä.



Kuvio 15: Vastaukset kysymykseen 9 - “Mitkä näet tärkeimpinä edellä esitetyistä hyödyistä? Ruksi kolme (3) kohtaa.”

5.3 Koetut haasteet

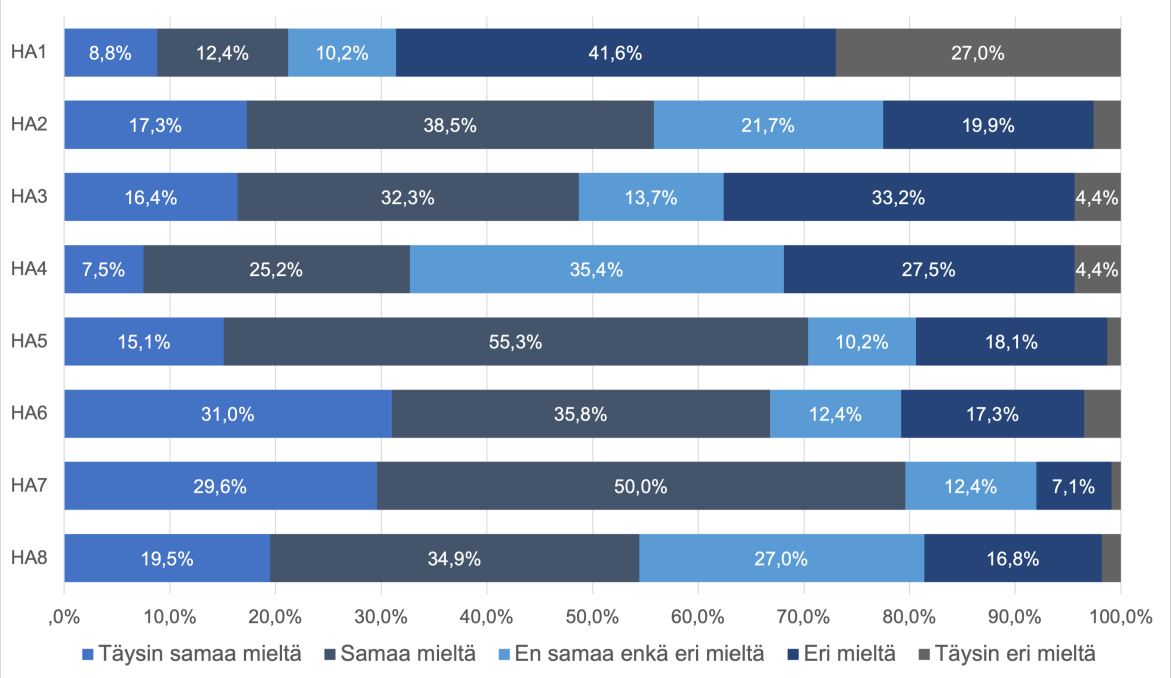
Koettujen haasteiden tulokset kysymykseen 11 on esitetty taulukossa 9. Mitä korkeampi tulosten keskiarvo oli, sitä suurempana haasteena vastaajat kokivat esitetyn väitteen. Käänteisesti, mitä matalampi keskiarvo oli, sitä pienempänä haasteena vastaajat kokivat väitteen. Vastauksien hajonta tässä haasteissa oli paljon suurempi hyödyissä. Keskiarvon mukaan suurimpana uhkana vastaajat kokivat haasteen HA7. Tämän jälkeen suurina uhkina koettiin haasteet HA6, HA5, HA8 ja HA2. Näissä haasteissa oli myös suurin mediaani (4.00). Vähiten uhkaavaksi koettiin haaste HA1. Tämän lisäksi myös haasteet HA4 ja HA3 koettiin vähemmän uhkaavina.

Koodi	Haaste	Keskiarvo	Mediaani	Keskihajonta
HA1	Digitaalinen henkilöllisyystodistus vaatii älylaitteen toimiakseen	2.35	2.00	1.25
HA2	Tunnusten palautus uudessa digitaalisessa henkilöllisyydessä voi olla vaikeaa, mikäli käyttäjä hukkaa tunnuksensa tai unohtaa salasanansa	3.48	4.00	1.25
HA3	Uuden henkilöllisyystodistuksen käyttö voi lisätä epäoikeudenmukaisuutta, sillä kaikilla ei välttämättä ole tarvittavia laitteita tai kykenevyyttä sen käyttöön	3.23	3.00	1.20
HA4	Suomen digitaalisessa henkilöllisyystodistuksessa käytetyt teknologiat ovat uusia, eikä niitä ole vielä tutkittu kattavasti	3.04	3.00	1.00
HA5	Joillain käyttäjillä voi olla vaikeuksia uuden henkilöllisyystodistuksen hallintaan tarkoitetun sovelluksen käytössä	3.65	4.00	0.99
HA6	Puhelimeni joutuessa vääriin käsiin, myös henkilöllisyystodistukseni vaarantuu	3.73	4.00	1.17
HA7	Uusi henkilöllisyystodistus voi tuoda mukanaan uusia tietoturvariskejä, joita ei vanhojen menetelmien kanssa ilmennyt	4.00	4.00	0.89
HA8	Uuden henkilöllisyystodistuksen väärinkäytön tai varkauden selvittäminen voi olla haastavaa, sillä henkilöllisyystodistuksen käytöstä ei tallennu tietoa	3.54	4.00	1.04

Taulukko 9: Vastaukset kysymykseen 11: “Ilmoita, missä määrin olet samaa mieltä seuraavista väittämistä uuden digitaalisen henkilöllisyystodistuksen suhteen.”

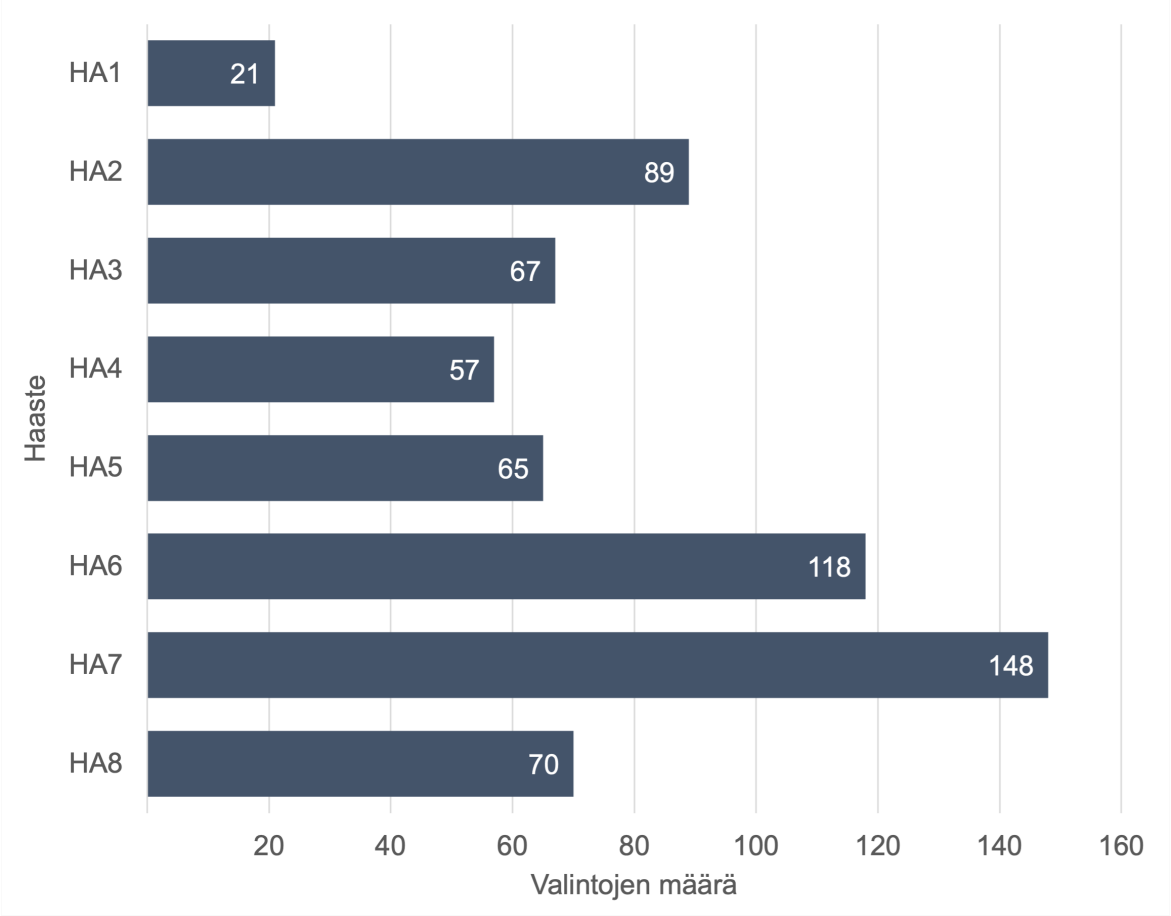
Kuviossa 16 on esitetty vastausten tarkempi jakautuminen kysymykseen 11. Tuloksista voi-

daan huomata, että vastaukset ovat jakautuneet melko laajasti vastausvaihtoehdoittain. Kuitenkin, “Täysin eri mieltä” -vaihtoehtoa ei ole vastattu kovin paljoa lukuun ottamatta haastetta HA1. Vastaajat ovat olleet myös enemmän samaa mieltä väittämien kanssa, kuin eri mieltä.



Kuvio 16: Vastaukset kysymykseen 11 – Jakautuminen vastauksittain

Kuviossa 17 esitellään olennaisimmiksi koetut haasteet. Tämän mukaan haaste HA7 on koettu selkeästi olennaisimmaksi. Toiseksi olennaisimmaksi haasteeksi taas koetttiin HA6 ja kolmanneksi haaste HA2. Haasteet HA3, HA4, HA5 sekä HA8 saivat melko tasaisesti vastauksia. Selkeästi vähiten olennaiseksi koettiin haaste HA1. Tarkastellessa kysymysten 11 ja 12 tuloksia yhdessä voidaan huomata, että haaste HA7 koettiin suurimpana uhkana kummankin kysymyksen tuloksissa. Toisiksi suurimmaksi uhaksi koettiin haaste HA6.



Kuvio 17: Vastaukset kysymykseen 12: “Mitkä näet tärkeimpinä edellä esitetyistä hyödyistä? Ruksi kolme (3) kohtaa.”

5.4 Avointen kysymysten vastaukset

Kyselyssä oli kaksi avointa kysymystä: “Onko jotain muuta, minkä toteutumisen tai huomioon ottamisen uudessa henkilöllisyystodistuksessa koet tärkeäksi?” (kysymys 10) ja “Onko jotain muuta, minkä koet haasteelliseksi tai mistä olet huolissasi uuden henkilöllisyystodistuksen suhteen?” (kysymys 12).

Useissa ensimmäisen kysymyksen vastauksissa esiintyvä teema oli SSI:n helppokäyttöisyyden sekä saavutettavuuden tärkeys. Tämän lisäksi useissa vastauksissa esiintyi myös hyvän tietoturvan toteutumisen tärkeys. Muita esiintyneitä teemoja olivat fyysisen henkilökortin säilyminen uuden todistuksen rinnalla, itsehallittavuus sekä huoli mahdollisen väärinkäytön

seuraamisesta. Ensimmäiseen kysymykseen vastattiin seuraavilla tavoilla:

> Kuinka kortin väärinkäyttöä tullaan seuraamaan. Esim estetäänkö henkilökortista näyttökuvan ottamista ja kuvan jakamista? Yleistyvätkö alaikäisillä täysi-ikäisten henkilökorttien väärinkäyttö esim alkoholin ja tupakan ostamisessa?
>
> Tieto pysyy luotettavampana ja päivitettävänä. Uutta henkilöllisyystodistusta ei toivottavasti pysty jakamaan toiselle henkilölle kuten perinteisiä henkkareita.
>
> Digitaalinen versio olisi vain vaihtoehto, ei pakko.
>
> Helppokäyttöisyys (x2)
>
> Toimimisen sujuvuus on mielestäni tärkeää, kuten tietoturva. Itsehallittavuus tärkeää, esimerkiksi tunnistautuessa tuleva boksi jossa kysyttäisiin “missä laajuudessa haluat palveluntarjoajan näkevän tietosi ?” Ja siihen mahdollisuus tehdä pikavalintoja. Toisaalta triviaalimmissa asioissa kuten viinan ostossa tms niin voisi olla vaan että “palveluntarjoaja saa tietää sinusta seuraavat tiedot” ja luettelo perään. Lisäisi kivasti läpinäkyvyyttä. Mutta täysin uusi juttu mulle tämä kokonaan.
>
> Käyttöönotto on vaivatonta ja sovellus tarpeeksi simppeli
>
> Digitaalisen henkilöllisyystodistuksen käyttöönotto yksityisen sektorin palveluille tulisi olla mahdollisimman helppoa ja kustannustehokasta, jotta se tulisi nopeasti ja laajasti käyttöön.
>
> Rajat ylittävä tunnistaminen sähköisessä asioinnissa EU:n sisällä.
>
> Tietoturvan, koska tuntuu ettei mikään ole kyberuhkien takia turvassa nykyisin.
>
> Tietoturva toteutuu
>
> Varmistaa, että onnistuu myös vanhuksilta ja henkilöiltä keillä IT taidot tai kielitaito puutteellinen
>
> Se lisäksi että on mahdollista päättää mitä tietoja jaan ja miten niitä hyödynne-

> tään, näiden valintojen tekeminen pitää olla hyvin helppoa ja selkokielistä.
>
> Ei saa olla syrjivä järjestelmä niitä kohtaan jotka eivät pysty käyttämään älylaitteita. Rinnalla on kuljettava tasavertaisena perinteinen menetelmä.

Jälkimmäisen kysymyksen vastauksissa taas esiintyi huoli siitä, miten toimitaan, kun mobiililaite ei ole käytössä esimerkiksi akun loppumisen takia. Tätä haastetta ei ollut esitetty kysymyksen 10 väittämissä, joten se oli uusi löydös vastauksista. Samaiseen teemaan osuivat huolet siitä, miten toimitaan, kun ei ole mobiililaitetta saatavilla tai sen käyttöön ei ole kykenevyyttä. Tämä koettiin huoleksi etenkin vanhemman sukupolven puolesta. Huoli esiintyi myös siitä, ettei digitaalisen henkilöllisyystodistuksen sovellus tukisi muita kuin iOS- ja Android-käyttöjärjestelmiä, tai näiden käyttöjärjestelmien vanhempia versioita.

Kysymykseen 12 vastattiin seuraavilla tavoin:

> Tuntuu, että olisi pakko pitää rinnalla myös normaalia henkkaria, jos loppuu akku / puhelin hajoaa tmv. Olisko sillok digitaalisesta hyötyä?
>
> Tunnusten palautukseen tms pitäisi olla vain tosi foolproof menetelmä irlin puolella
>
> Jos ei ole akkua laitteessa, miten sitten toimitaan?
>
> Vanhempi ikäpolvi ei varmasti kykene ottamaan haltuun asioita samaan malliin kuin nuoremmat
>
> Siitä, miten monet uudistukset kannustavat puhelimen jatkuvaan käyttöön eivätkä anna ihmisille mahdollisuutta pian enää omistaa esimerkiksi sellaista puhelinta, joka soveltuu vaan soittamiseen ja viestien lähettämiseen. Myöskin tällaisten uudistuksien tulisi mielestäni tukea vanhempia versioita käyttöjärjestelmistä, eikä pakottaa ihmisiä esimerkiksi ostamaan uusia puhelimia, vaan koska heidän IOS tai Android käyttöjärjestelmänsä ei enää ole päivitettävissä vanhassa mallissa eikä siksi uusi sovelluskaan toimi (tai miten tämä identiteetti nyt sitten toteutetaan). Tämä antaisi liikaa valtaa yksityisille yrityksille pakottaa ihmisiä jatkuvaan kulutukseen ja lisäisi epäarvoisuutta, sillä kaikilla ei ole

jatkuvasti varaa päivittää puhelintaan uusimpaan malliin. Lisäksi tällaisten järjestelmien pettäminen voi olla huolestuttavaa, jos olemassa ei ole varasuunnitelmaa siitä, miten sitten yhteiskunnan tulisi toimia.

Kuinka moni tulee todellisuudessa sen ottamaan käyttöön, jos palveleva taho ei hyväksy digitaalista henkkaria.

Ihmettelen miksei henkilökorttia oteta käyttöön Applen ja Googlen tarjoamilla toiminnoilla. Apple lanseerasi jokin aika sitten oman digitaalisen henkilökorttinsa joka toimii hyvin samalla periaatteella kuin suomalaisten oma. Uskon kuitenkin, että koska Applella on huomattavasti parempi kontrolli ja suuremmat satsaukset tämän kaltaiseen palveluun heidän ratkaisunsa on luultavasti turvallisempi, helpompi käyttää ja tehokkaampi ottaa käyttöön. Googlella sama juttu. Ihmettelen suomalaisten tarvetta tehdä itse jotain mihin laitteiden valmistajat ovat jo keksineet toimivat ratkaisut. En usko siihen että suomalaiset virastot osaisivat asiaa tehdä paremmin ja siksi olen hieman skeptinen hankkeen suhteen vaikkakin uskon tämän olevan todella tervetullut askel yhteiskuntamme digitalisaatiossa

Tietoturvariskit

Epäoikeudenmukaisuus tulee kuvaan sitten, jos vanha henkilöllisyystodistus tai muut nykyiset tunnistautumistavat eivät enää kelpaa.

Häiriöt tietoteknisissä järjestelmissä.

Miten epäoikeudenmukaisuus lisääntyy jos ihmisille tarjotaan uusi henkilöllisyystodistusmuoto? Vanhat tavat oletettavasti säilyy rinnalla. Kehityksen jarruna ei voi olla vähemmistön kykenemättömyys vaan kehitystä tulisi edistää enemmistö. Sitten voi muita vaihtoehtoisia keinoja tarjota niille, joilla ei ole kykyä tai mahdollisuutta käyttää digitaalisia välineitä. Toinen asia, jota jäin pohtimaan, on tuo “käytöstä ei tallennu tietoa”. Onko tosiaan näin? Jos kirjaannun pankkiin tai omakantaan niin eikö edelleen nuo järjestelmät loggaa kirjautumista? Toisaalta jos käytän digitunnusta vaikka baarin ovella niin eihän siitä

nytkään jälkeä jää. Mikä tuon osalta siis muuttuu nykyiseen verrattuna?

Digitaalinen henkilötodistus ei sovellu kaikille käytettäväksi (laite, osaamista nen), vaan vanhojen fyysisten tunnistusmenetelmien tulee olla edelleen sujuvasti käytettäviä.

5.5 Eksploratiivinen faktorianalyysi

Aineistolle suoritettiin SPSS-ohjelmistolla faktorianalyysi käyttäen principal axis factoring -menetelmää ja direct oblimin -rotaatiota. Analyysi tehtiin ensin kysymyksistä 8 ja 11 saaduille muuttujille eli hyödyille ja haasteille. Metsämuurosen (2011, s. 670) mukaan yksittäisten muuttujien kommunaliteetit tulisivat olla yli arvon 0,3, jotta ne kannattaa sisällyttää tutkimukseen. Muuttujien HY4, HY6, HA2 ja HA5 kommunaliteetit jäivät tämän raja-arvon alapuolelle, jonka takia ne jätettiin analyysin ulkopuolelle. Tämän jälkeen faktorianalyysi ajettiin uudelleen, jolloin kaikkien muuttujien kommunaliteetit olivat yli kyseisen raja-arvon.

Kommunaliteetin lisäksi tärkeitä faktorianalyysissä huomioitavia asioita ovat riittävän suuri otoskoko sekä tarpeeksi vahvat faktorilataukset (Yong, Pearce ym. 2013). Yong, Pearce ym. (2013) mukaan riittävä otoskoko on 300 henkilöä, ja tällä otannalla riittävä faktorilataus on 0,32. Guadagnoli ja Velicer (1988) sanoo pienemmänkin otoskoon riittävän vahvemmalla faktorilatauksella. He mainitsevat 0,6 faktorilatauksen olevan riittävä 150 henkilön otannalla. Tässä tutkimuksessa faktorilatauksen raja-arvoksi valittiin 0,48, jotta kaikista saaduista faktoreista johdettavat ryhmät olivat mielekkäitä. Tämä nähtiin perusteltuna, sillä tutkimuksen 226 henkilön otoskoko on selvästi Guadagnolin ja Velicerin rajan yläpuolella, vaikka ei ylläkään Yongin ja Pearcenin 300 henkilön rajaan. Raja-arvon alle jääneet faktorilataukset jätettiin pois taulukosta. Lopullinen rotatoitu faktorimatriisi on esitelty taulukossa 10.

	1	2	3	4
HY1	0.788			
HY2	0.871			
HY3	0.656			
HY5	0.650			
HY7			0.628	
HY8			0.826	
HY9			0.580	
HY10			0.569	
HA1				0.487
HA3				0.835
HA4		0.603		
HA6		0.759		
HA7		0.674		
HA8		0.646		

Taulukko 10: Rotatoitu faktorimatriisi

Tulosten saamisen jälkeen saatuja faktoreita ja niiden sisältämiä muuttajia analysoitiin. Tässä pyrittiin etsimään yhteneväisyyksiä faktorien sisältämien muuttujien välillä ja tätä kautta nimeämään saatuja faktoreita. Alla on esitelty analysoinnin tuloksena johdetut faktorien nimet taulukon 10 järjestyksessä:

1. Hyödyt: tietoturva ja yksityisyys (HY1, HY2, HY3, HY5)
2. Haasteet: tietoturva ja yksityisyys (HA4, HA6, HA7, HA8)
3. Hyödyt: käytettävyys ja saavutettavuus (HY7, HY8, HY9, HY10)
4. Haasteet: saavutettavuus (HA1, HA3)

6 Johtopäätökset ja pohdinta

Tässä luvussa käsitellään tutkimuksen tuloksia alan aiemman tutkimuksen valossa. Aluksi tutkimustuloksia käsitellään teorian näkökulmasta. Systemaattisen kirjallisuuskartoituksen ja kyselytutkimuksen tuloksia käsitellään tarkastellaan tässä erillisinä osioina. Tämän jälkeen tutkimusten tuloksia käsitellään kokonaisuutena käytännön näkökulmasta. Lopuksi pohditaan tutkielman rajoitteita ja mahdollisia jatkotutkimusaiheita.

6.1 Tutkimustulokset ja niiden teoreettiset kontribuutiot

Tutkielmassa suoritettiin kaksi tutkimusta: systemaattinen kirjallisuuskartoitus ja kyselytutkimus. Systemaattisella kirjallisuuskartoituksella pyrittiin vastaamaan seuraaviin tutkimuskysymyksiin: “Mikä on itsehallittavan identiteetin määritelmä ja mitkä ovat sen tärkeimmät komponentit?” ja “Mitä potentiaalisia hyötyjä ja haasteita itsehallittavaan identiteettiin liittyy käyttäjän näkökulmasta?”. Kyselytutkimuksella taas pyrittiin vastaamaan kysymykseen: “Mitkä ovat olennaisimmat itsehallittavan identiteetin hyödyt ja haasteet Suomen digitaalisen henkilöllisyystodistuksen kontekstissa loppukäyttäjän näkökulmasta?”. Seuraavissa kappaleissa esitellään tutkimusten tuloksia ja pohditaan näiden kontribuutiota SSI:n tutkimukselle.

6.1.1 Systemaattinen kirjallisuuskartoitus

Systemaattisen kirjallisuuskartoituksen potentiaalisten hyötyjen ja haasteiden tuloksille tehtiin kategorisointi. Hyödyille määritellyt kategoriat ja niiden esiintymät artikkeleissa olivat seuraavat: yksityisyys (62 kpl), turvallisuus (40 kpl), käytettävyys (32 kpl), resurssien säästäminen (8 kpl) ja sekalainen (8 kpl). Yksittäisistä hyödyistä eniten mainintoja artikkeleissa oli seuraavilla: *käyttäjällä on täysi kontrolli omasta identiteetistään* (23 kpl), *yksityisyyden turva (privacy)* (21 kpl) ja *tietoturva (data protection/security)* (20 kpl). Haasteiden kategoriat ja niiden esiintymät artikkeleissa taas olivat seuraavat: tekniset haasteet (33 kpl), kehityksen ja standardien puute (29 kpl), turvallisuuden ja yksityisyyden haasteet (18 kpl), luottamuksen haasteet (15 kpl), sekalaiset haasteet (15 kpl), kulujen nousu (13 kpl), käy-

tettävyyden haasteet (9 kpl) ja muutosvastahakoisuus (8 kpl). Haasteissa ei esiintynyt mitään yksittäistä haastetta, jolla olisi ollut selvästi muita enemmän esiintymiä. Hieman muita enemmän esiintymiä sisältäneet haasteet olivat kuitenkin seuraavat: *tunnusten (avaimen) palautus* (18 kpl), *standardien ja yhteisymmärryksen puute* (14 kpl), *"luottamusankkurin" puute* (11 kpl) ja *vaatii suuria muutoksia organisaatioissa ja infrastruktuureissa* (10 kpl). Kartoituksen tekemisen hetkellä SSI:n hyötyjä ja haasteita kartoittavaa systemaattista kirjallisuuskartoitusta ei ollut tehty, joten nämä tulokset ovat uutta tietoa SSI:n tieteenhaaralla.

Määritelmän suhteen kartoituksesta kävi ilmi, ettei selkeää konsensusta SSI:n määritelmästä vielä ole. Määritelmien analysoinnissa nousi esiin kolme eri tapaa, miten SSI:tä määriteltiin artikkeleissa: SSI paradigmana, SSI identiteetinhallintajärjestelmänä ja SSI digitaalisen identiteetin muotona. Näistä kaksi ensimmäistä olivat selvästi yleisempiä määritelmiä SSI:lle kuin SSI digitaalisen identiteetin muotona. Kaikissa SSI:n määritelmien tyypeissä yhtenevinä piirteinä SSI:lle nähtiin olevan etenkin käyttäjän täysi hallinta omasta identiteetistään sekä kolmannen osapuolen poistuminen identiteetinhallinnasta. Kartoituksessa kerättiin myös tietoa siitä, mihin muihin tutkimuksiin viitattiin SSI:n määritelmää esitellessä. Näistä selvästi eniten viitattiin Christopher Allenin artikkeliin *The Path to Self-Sovereign Identity* (2016). Kartoituksesta ilmenneet SSI:n keskeisimmät komponentit olivat seuraavat: *DID*, *VC*, *PKI*, *DLT*, *luottamuksen kolmio*, *digitaalinen lompakko*, *tietovarasto*, *ZKP*, *verifioitavissa oleva tietorekisteri* ja *älysopimukset*. Näistä selvästi esiintyneimmät olivat DID ja VC. Tämän oli odotettavissa, sillä ne ovat W3C:n kehittämiä standardeja. Myös PKI, DLT, luottamuksen kolmio ja digitaalinen lompakko esiteltiin useasti SSI:n komponentteina.

Aiempaa SSI:n komponentteja ja sen määritelmää tarkastelevaa tutkimusta on jo tehty, mutta näissä tehdyt kartoitukset eivät ole olleet systemaattisia. Esimerkiksi Mühle ym. (2018) tutkimus oli toiseksi viitatuin artikkeli tämän kartoituksen tuloksissa, ja sen tutkimuskohteena oli SSI:n arkkitehtuuri sekä sen sisältämät komponentit. He määrittelivät SSI:n koostuvan seuraavista komponenteista: *identifiointi*, *autentikointi*, *todennettavissa olevat väitteet* ja *tietovarasto*. Kyseinen jaottelu tarkastelee SSI:tä abstraktimmalla tasolla. Tässä tutkimuksessa selvinneet komponentit ovat enemmän käytännön tason teknologioita, vaikka joitakin abstraktimpia komponentteja, kuten luottamuksen kolmio sekä verifioitavissa ole-

va tietorekisteri, myös ilmeni. Tutkimusmenetelmän lisäksi myös tarkastelun tason suhteen Mühle ym. (2018) tutkimukseen verraten on siis eroavaisuuksia.

Myös Shuaib, Hassan, Usman, Alam, Bhatia, Agarwal ym. (2022) antavat artikkelissaan kattavan määritelmän ja kuvauksen SSI:n arkkitehtuurista sekä sen sisältämistä komponenteista. He laskevat seuraavat komponentit osaksi SSI:tä: *DID*, *VC*, *VP*, *digitaalinen lompakko*, *valtuustietojen varmentajat (engl. certificate authorities)*, *DLT* sekä *identifiointi, autentikointi ja auktorisointi*. Näistä komponenteista valtaosa ilmeni tässäkin tutkimuksessa SSI:n komponenteiksi, mutta eroavaisuuksiakin tähän tutkimukseen verraten oli. Kyseinen tutkimus ei myöskään ollut systemaattinen kirjallisuuskartoitus, jonka takia sen jaottelu komponteista on enemmän kyseisten tutkijoiden näkemys SSI:n komponenteista. Kyseisessä tutkimuksessa mentiin komponenttien analysoinnissa kuitenkin vielä hieman pidemmälle; siinä analysoitiin, miten kukin komponentti edistää Allenin (2016) esittämien SSI:n ohjenuorien toteutumista.

SSI:hin liittyviä systemaattisia kirjallisuuskartoituksia on myös tehty (Siqueira, Da Conceição ja Rocha 2021; Shuaib, Hassan, Usman, Alam, Bhatia, Mashat ym. 2022; Cucko ym. 2022; Schardong ja Custódio 2022), mutta näillä on ollut eri tutkimuskohteet. Mikään tutkielman kirjoittamisen aikaan tehty tutkimus ei siis vastannut tätä tutkimusta sekä siinä käytetyn tutkimusmenetelmän, että sen tutkimuskohteen puolesta. Tulokset SSI:n määritelmän ja sen sisältämien komponenttien suhteen voidaan siis katsoa olevan uusia SSI:n tutkimukselle.

6.1.2 Kyselytutkimus

Kyselytutkimuksen tuloksista huomattiin, että loppukäyttäjät kokevat paremman tietoturvan ja yksityisyyden sekä itsehallittavuuden tärkeimpinä hyötyinä. Avoimet vastaukset tukevat näitä tuloksia tuoden kuitenkin myös saavutettavuuden edellä mainittujen teemojen lisäksi. Loppukäyttäjät kokevat selkeästi uhkaavimmiksi tietoturvaan liittyvät haasteet sekä varastamiseen, unohtamiseen ja väärinkäyttöön liittyvät haasteet. Lisäksi käyttäjät kokevat vaikeakäyttöisyyden ja teknologian kehityksen puutteen jokseenkin suurena uhkana. Uhkaavimmiksi koetut teemat eivät nousseet esiin avoimissa vastauksissa muita haasteita enemmän, mutta mainintoja niistä esiintyi. Haaste siitä, mitä tehdään, kun älylaitteen akku

loppuu tai sen toiminta vain lakkaa, nousi esiin avoimissa vastauksissa useaan otteeseen. Kyseistä haastetta ei ollut mainittu kyselytutkimuksen muissa kysymyksissä, eikä se noussut suoranaisesti esiin kirjallisuuskartoituksessa, joten se voidaan nähdä uutena löydöksenä.

Tietoturva nähtiin yhtenä tärkeimmistä hyödyistä, mutta samalla suurimpana haasteena. Tämä on sinänsä ristiriitaista, mutta toisaalta myös ymmärrettävää, sillä kumpikin tulos viittaa siihen, että tietoturva on tärkeä teema loppukäyttäjille. Sekä hyödyissä, että haasteissa helppokäyttöisyys nähtiin tärkeänä tai vaikeakäyttöisyys uhkaavana. Hyödyt ja haasteet kuitenkin erosivat toisistaan muissa teemoissa. Lisäksi eksploratiivisen faktorianalyysin avulla hyödyt ja haasteet saatiin jaoteltua neljään eri ryhmään: Tietoturvaan ja yksityisyyteen liittyvät hyödyt, tietoturvaan ja yksityisyyteen liittyvät haasteet, käytettävyyteen ja saavutettavuuteen liittyvät hyödyt sekä saavutettavuuteen liittyvät haasteet. Ryhmien jakautuminen oli suhteellisen luontevaa, sillä kysymyksistä erottui selkeitä yhteneviä teemoja jo kirjallisuuskartoituksessa.

Tutkimusta, joka olisi tutkinut SSI:n koettuja hyötyjä sekä haasteita loppukäyttäjän näkökulmasta, ei löytynyt tutkielman kirjoittamisen aikaan. Sen sijaan Laatikainen, Kolehmainen ja Abrahamsson (2021) tutkivat näitä koettuja hyötyjä sekä haasteita asiantuntijoiden ja ammattilaisten näkökulmasta, joille SSI käsitteenä ja käytäntönä oli jo ennestään tuttu. He esittivätkin tutkimuksessaan, että loppukäyttäjien näkemyksiä tulisi tutkia samassa kontekstissa heidän tutkimuksensa jatkoksi. Tämä tutkielma vastaa tähän jatkotutkimusehdotukseen. Laatikainen, Kolehmainen ja Abrahamsson (2021) esittävät samat hyödyt ja haasteet tutkimuksessaan, kuin tämän tutkimuksen tärkeimmäksi koetut hyödyt ja haasteet. He eivät kuitenkaan ole vertailleet näitä hyötyjä ja haasteita sekä niiden tärkeyttä keskenään. He ovat myös jakaneet hyödyt ja haasteet yritysten hyötyihin ja haasteisiin sekä yhteiskunnalle koituviin hyötyihin ja haasteisiin. Tuloksia ei siis voi suoraan verrata tämän tutkimuksen tuloksiin.

Kankaan (2022) pro gradu -tutkielma tutki digitaalisen lompakon omaksumiseen vaikuttavia tekijöitä SSI:n kontekstissa. Tutkielma keskittyi verkkokauppa-asioinnin yhteyteen ja enemmän juurikin digitaaliseen lompakkoon, joka on SSI:n osa-alue. Kuitenkin, tutkielmassa löydetyt tulokset digitaalisen lompakon omaksumiselle sisälsivät paljon samoja teemoja, kuin tämän tutkimuksen hyödyt ja haasteet. Näitä teemoja olivat esimerkiksi turvalli-

suus, tietojen hallinta ja helppokäyttöisyys. Myöskään tässä tutkimuksessa näitä tekijöitä ei oltu vertailtu keskenään, vaan listattu vain kokonaisuudessaan.

Näiden asioiden pohjalta voidaan todeta tutkimuksesta esiin nousseiden hyötyjen ja haasteiden olevan pitkälti samoja, kuin mitä aiemmassa tutkimuksessa on esiintynyt. Tämä tutkimus siis toimii näitä validoivana tutkimuksena. Täysin uutena tietona tämä tutkimus toi kuitenkin näiden hyötyjen ja haasteiden vertailemisen keskenään sekä niiden arvottamisen. Suorana eroavaisuutena on se, että kysely pohjautui Suomen digiuudistukseen sekä se, että siinä hyötyjä ja haasteita tarkasteltiin loppukäyttäjän näkökulmasta.

6.2 Tulosten merkitys käytäntöön

Tutkielman kirjallisuuskartoitus tarjoaa käytännön tason hyödyntämismahdollisuuksia komponenttien sekä hyötyjen ja haasteiden tulosten kautta. Kartoituksessa selvitettyjä SSI:n keskeisimpiä komponentteja voidaan käyttää pohjana SSI:n arkkitehtuurin luonnissa. Komponentit sisältävät käytännössä kaiken tarvittavan SSI:n toteutukselle ja siten myös arkkitehtuurin rungolle.

Esiin nousseita hyötyjä ja haasteita voidaan myös hyödyntää SSI:n käytännön toteutuksissa. Niistä voidaan ottaa mallia ja niitä voidaan käyttää sovelluksen arvioinnin apuna tarkistamalla, että siinä toteutuu esitetyt hyödyt, ja että siinä on otettu huomioon esitetyt haasteet. Kyselytutkimuksen hyötyjen ja haasteiden asettaminen tärkeysjärjestykseen auttaa tätä vielä entisestään. Kehitystyötä voidaan tämän avulla suunnata niihin osa-alueisiin, jotka ovat loppukäyttäjien kokevat tärkeimpinä. Tämän avulla voidaan allokoida resursseja olennaisimpien ominaisuuksien toteuttamiseen.

Lisäksi, koska kyselytutkimus käsitteli loppukäyttäjien näkemyksiä Suomen digitaalisesta henkilöllisyystodistuksesta, voisi sen tuloksia hyödyntää etenkin kyseisessä hankkeessa. Suomen digitaalinen henkilöllisyystodistus on tätä kirjoitelmaa kirjoittaessa vielä kehitysvaiheessa. Se tulee myös alkuperäisen lanseeraamisen jälkeen tarvitsemaan jatkuvaa päivitystä ja kehittämistä. Kyselytutkimuksen tulokset antavat näille prosesseille informaatiota siitä, mitä haasteita loppukäyttäjien näkökulmasta olisi olennaista ratkaista ja minkä hyötyjen pitäisi etenkin toteutua. Muissa kehityshankkeissa näitä tuloksia on tarkasteltava

kriittisesti ja sovellettava hankkeeseen sopivalla tavalla.

6.3 Rajoitteet

Aluksi käsitellään yleisiä rajoitteita. Koska tutkielma oli opinnäytetyö, johon tutkijoilla oli rajalliset resurssit käytössä, ja johon liittyi aikataulupaineita, voi jotkin tutkimuksen osa-alueet olla käyty hieman kiireellisesti läpi. Kyselyn jakamiseen käytettiin pääasiassa tutkijoiden omien sosiaalisten medioiden kanavia, sillä sitä ei ollut mahdollista jakaa maksullisten kanavien kautta, eikä vastauksia voitu odottaa pitkiä aikoja. Tämä voi heikentää kyselyn tulosten yleistettävyyttä. Käytetyt tutkimus- ja tilastomenetelmät olivat myös tutkijoille uusia, mikä on voinut johtaa tulosten vajanaiseen tulkintaan.

Kirjallisuuskartoituksesssa tavoitteena oli tutkia sekä SSI:n hyötyjä ja haasteita, että sen määritelmää. Pelkät haasteet, hyödyt tai määritelmä ei ollut yksin kartoituksen keskipisteenä. Tästä syystä kartoituksesta saattoi jäädä pois artikkeleita, jotka olisi laskettu määritelmän perusteella sisällytettäviksi, mutta jäivät ulos, koska niissä ei ollut esitelty hyötyjä ja haasteita. Lisäksi kirjallisuuskartoituksen edetessä tutkijoiden aihepiirin tietämys lisääntyi sekä tutkimusmenetelmän osaaminen kehittyi, mikä on voinut aiheuttaa eroavaisuuksia kartoitusprosessissa sen eri vaiheissa. Tutkielma toteutettiin kahden tutkijan toimesta, mikä myös saattoi aiheuttaa kirjallisuuskartoituksen artikkelien suodatusprosessissa eroavaisuuksia. Vaikka artikkelien arviointikriteerit oli määritelty tarkasti ja tutkijoiden tulkinta niistä pyrittiin pitämään samanlaisena, on silti mahdollista, että tutkijat päätyivät eri tuloksiin artikkeleita lukiessa.

Kyselytutkimuksen osalta kyselylomakkeen olisi voinut tehdä hieman paremmin. Esimerkiksi satunnaistamalla hyötyjen ja haasteiden väitteiden järjestystä kyselyssä oltaisiin mahdollisilta kysymysjärjestyksen aiheuttamilta vinoumilta voitu välttyä. Lisäksi, kyselyn yleistettävyyttä sekä demografiaryhmien välistä vertailtavuutta olisi myös voitu parantaa laajentamalla otantaa tai muuttamalla jakelukanavia.

Koska tutkimuksessa tutkitaan ihmisten asenteita jotain ilmiötä kohtaan, on mahdollisuus metodisille vinoumille (engl. common method bias). Metodinen vinouma on kyselytutkimuksen keräystavasta johtuva vääristymä tai systemaattinen mittausvirhe (Podsakoff

ym. 2003). Aiemmin mainittu kysymysten järjestyksen satunnaistamatta jättäminen on esimerkki kyselytutkimuksen keräystavasta johtuvasta vääristymästä. Systemaattisia mittausvirheitä saattoi syntyä tutkijoiden kokemattomuudesta mittaustyökaluihin liittyen tai mittareiden ja analyysityökalujen valinnoista johtuen.

6.4 Jatkotutkimus

Yleisesti SSI:n tutkimuksessa selvänä vajavaisuutena on empiirinen tutkimus. Tällä hetkellä tämä tutkimus on hyvin vähäistä, etenkin käytännön tason tarkastelussa. Suurin osa tämänhetkisestä SSI:n tutkimuksesta on erilaisia arkkitehtuuriehdotuksia, jonkin SSI:n teknisen ongelman ratkaisuehdotuksia tai SSI:n sovellutuksia. Myös käytännön ratkaisumallit tai työkalut SSI:n implementointiin ovat kohtuullisen yleisiä tutkimuskohteita. Näitä ovat esimerkiksi Sovrinin sekä uPortin valkoiset kirjat heidän SSI:n käytännön sovellutuksistaan. Näitä oikean maailman käytännön esimerkkejä on silti vain vähän ja niitä tutkivia tutkimuksia vielä vähemmän. Tästä syystä aihepiiri vaatisi lisää empiiristä tutkimusta ja esimerkiksi Case study -tyyppistä tutkimusta jonkin käytännön toteutuksen parissa. Tällaista tutkimusta tarvitaan, kun SSI alkaa yleistymään käytännössä, jotta kaikkia SSI:n potentiaalisia hyötyjä ja haasteita saadaan implementoitua käytännön tasoon.

Empiirisen tutkimuksen lisäksi SSI:n komponentit vaativat standardisointia. Ylipäänsä SSI:n arkkitehtuuri vaatii standardisointia ja sen komponenttien vakiintumista. SSI:n sisältö tulisi siis vakiinnuttaa kokonaisuudessaan, mutta myös yksittäiset komponentit tulisi standardisoida. Tällä hetkellä DID:lle ja VC:lle on olemassa omat standardinsa, mutta muilta komponenteilta nämä vielä puuttuvat. Osaksi tähän liitoksissa, myös itsehallittavan identiteetin määritelmä kokonaisuudessaan vaatii vielä selkeytystä. Määritelmälle on jo hyvä pohja ja tämäkin tutkimus on sitä määrittänyt, mutta se ei vielä ole täysin yhtenäinen ja alan tutkimusyhteisössä vakiintunut.

Tässä tutkielmassa toteutettu kyselytutkimus kohdistui resurssiensa puitteissa suhteellisen pienelle kohderyhmälle, jonka takia sitä ei voida yleistää koskemaan koko Suomen kansaa. Saman tyylinen tutkimus tulisi toteuttaa isommalle otannalle ja isommalla mittakaavalla, jotta tuloksia voitaisiin yleistää paremmin suurempaan populaatioon. Lisäksi tutkimusta

voisi laajentaa käsittelemään kaikkia SSI implementaatioita yleisesti. Silloin tuloksia voisi paremmin verrata kaikkiin SSI:n käyttökohteisiin. Tietenkin tämä vaatisi tutkimukseen osallistuvilta jonkinlaista ymmärrystä aihepiiristä, sillä sitä ei voisi silloin liittää mihinkään konkreettiseen sovellutukseen, kuten Suomen digiuudistukseen tämän tutkimuksen tapauksessa.

7 Yhteenveto

Tämän tutkielman tarkoituksena oli selvittää SSI:n määritelmää, sen keskeisimpiä komponentteja sekä tarkastella sen sisältämiä potentiaalisia hyötyjä ja haasteita. Tutkielma koostui kahdesta tutkimuksesta: systemaattisesta kirjallisuuskartoituksesta ja kyselytutkimuksesta. Kirjallisuuskartoituksessa tarkasteltiin SSI:n määritelmää ja sen keskeisiä komponentteja sekä pyrittiin selvittämään kokonaisuudessaan SSI:hin liittyviä potentiaalisia hyötyjä ja haasteita. Kyselytutkimuksessa taas tarkasteltiin mahdollisten loppukäyttäjien näkemyksiä Suomen uuden, itsehallittavaan identiteettiin pohjautuvan, digitaalisen henkilöllisyystodistuksen hankkeesta.

Kirjallisuuskartoituksesta käsitellessä kävi ilmi, että SSI:n tutkimuksessa puuttuu vielä yleinen konsensus sen määritelmästä. Esiintyneet määritelmät jaettiin kolmeen tyyppiin: SSI paradigmana, SSI identiteetinhallintajärjestelmänä ja SSI digitaalisen identiteetin muotona. Kaikille näille tyypeille esiintyi jaettuina piirteinä käyttäjän täysi kontrolli omasta identiteetistään sekä kolmannen osapuolen eliminointi identiteetinhallinnasta. Keskeisimpiä komponentteja SSI:lle olivat selvästi DID ja VC. Näiden lisäksi SSI:n komponentteina nähtiin useasti myös PKI, DLT, luottamuksen kolmio ja digitaalinen lompakko. Myöskään siinä, lukuun ottamatta DID:tä ja VC:tä, mistä komponenteista SSI koostuu, ei ole vielä selkeää yhteisymmärrystä. Tämä näyttää vaihtelevan muun muassa sen mukaan, mihin kontekstiin SSI:tä ollaan soveltamassa.

SSI:n potentiaalisista hyödyistä loppukäyttäjät kokivat tärkeimpinä tietoturvan ja yksityisyyden kehittymisen sekä täyden kontrollin omista tiedoistaan. Yleisesti katsoen kaikki hyödyt koettiin kuitenkin tärkeiksi eli selkeää eroa tulosten välillä ei ollut. Haasteiden näkemyksissä eroavaisuuksia taas oli enemmän. Loppukäyttäjät kokivat selkeästi uhkaavimmiksi tietoturvaan, identiteettivarkauteen, tunnusten palauttamiseen sekä identiteettitietojen mahdolliseen väärinkäyttöön liittyvät haasteet. Uutena haasteena tuloksissa ilmeni huoli siitä, miten toimitaan, kun älylaitteen akku loppuu.

Suurimpana rajoitteena tutkielmalle olivat rajalliset resurssit. Tästä syystä kyselyä ei muun muassa voitu jakaa erittäin suurelle joukolle, minkä takia otanta on melko vähäinen ja koh-

deyleisöltään rajoittunut. Tämän takia kyselyn tulokset eivät välttämättä ole yleistettävissä, eikä eri demografiaryhmien välistä vertailua voida tehdä niille hyvin. Kyselytutkimukselle spesifinä rajoitteena oli kysymysjärjestyksen satunnaistamisen puuttuminen. Tämä on voinut muuttaa joidenkin hyötyjen tai haasteiden arvottumista sen mukaan missä kohdassa väittämä on esiintynyt. Systemaattiselle kirjallisuuskartoitukselle spesifinä rajoitteena taas oli mahdollisuus eroavaisuuksille suodatus- ja ekstraktointiprosesseissa kahden tutkijan välillä. Tätä pyrittiin kuitenkin välttämään validoimalla yhteisymmärrystä valintakriteereistä useampaan otteeseen ennen lopullisen artikkelien suodatuksen tekemistä.

Jatkotutkimusmahdollisuuksia ja -tarvetta SSI:hin liittyen on usealla saralla. SSI:tä tulisi tutkia lisää käytännön käyttötapauksien kautta. Etenkin käytännön tason empiiriselle tutkimukselle olisi tarve. Myös kattavammalle standardisoinnille, etenkin sen arkkitehtuuriin ja komponentteihin liittyen, olisi tarvetta.

Lähteet

Ali, Muneeb, Jude Nelson, Ryan Shea ja Michael J Freedman. 2016. “Blockstack: A global naming and storage system secured by blockchains”. Teoksessa *2016 USENIX annual technical conference (USENIX ATC 16),* 181–194.

Allen, C., A. Brock, V. Buterin, J. Callas, D. Dorje, C. Lundkvist, P. Kravchenko, J. Nelson, D. Reed, M. Sabadello ym. 2015. *Decentralized public key infrastructure. A White Paper from Rebooting the Web of Trust.* Tekninen raportti.

Allen, Christopher. 2016. “The path to self-sovereign identity”.

Bai, P., S. Kumar, G. Aggarwal, M. Mahmud, O. Kaiwartya ja J. Lloret. 2022. “Self-Sovereignty Identity Management Model for Smart Healthcare System”, https://doi.org/10.3390/s22134714.

Bai, Pinky, Sushil Kumar, Geetika Aggarwal, Mufti Mahmud, Omprakash Kaiwartya ja Jaime Lloret. 2022. “Self-sovereignty identity management model for smart healthcare system”. *Sensors* 22 (13): 4714.

Benet, Juan. 2014. “Ipfs-content addressed, versioned, p2p file system”. *arXiv preprint arXiv:1407.3561*.

Buchmann, Johannes, Evangelos Karatsiolis, Alexander Wiesmaier ja Evangelos Karatsiolis. 2013. *Introduction to public key infrastructures.* Nide 36. Springer.

Cameron, Kim. 2005. “The laws of identity”. *Microsoft Corp* 12:8–11.

Camp, JL. 2004. “Digital identity”. *IEEE Technology and society Magazine* 23 (3): 34–41.

Check, Joseph, ja Russell K Schutt. 2012. “Survey research”. Teoksessa *Research methods in education,* 159–185. Sage publications.

Christidis, Konstantinos, ja Michael Devetsikiotis. 2016. “Blockchains and smart contracts for the internet of things”. *Ieee Access* 4:2292–2303.

Creswell, John W. 2014. “Quantitative methods”. Teoksessa *Research design: Qualitative, quantitative, and mixed methods approaches,* 200–230. Sage publications.

Cucko, S., S. Becirovic, A. Kamisalic, S. Mrdovic ja M. Turkanovic. 2022. “Towards the Classification of Self-Sovereign Identity Properties”, 88306–88329. https://doi.org/10.1109/ACCESS.2022.3199414.

Čučko, Špela, Šeila Bećirović, Aida Kamišalić, Saša Mrdović ja Muhamed Turkanović. 2022. “Towards the classification of Self-Sovereign Identity properties”. *IEEE Access* 10:88306–88329.

Dib, Omar, ja Khalifa Toumi. 2020. “Decentralized identity systems: architecture, challenges, solutions and future directions”. *Annals of Emerging Technologies in Computing (AETiC), Print ISSN,* 2516–0281.

DVV, Digi- ja väestövirasto. 2023. “Digitaalisen henkilöllisyyden uudistus, 2023, Accessed: 2023-02-22”. Viitattu 22. helmikuuta 2023. https://dvv.fi/digitaalisen-henkilollisyyden-uudistus.

Ebrahimi, A. 2019. “Identity management verified using the blockchain”. *ShoCard, Tech. Rep.*

El Ioini, Nabil, ja Claus Pahl. 2018. “A review of distributed ledger technologies”. Teoksessa *OTM Confederated International Conferences"On the Move to Meaningful Internet Systems",* 277–288. Springer.

Ellis, James H. 1970. “The possibility of secure non-secret digital encryption”. *UK Communications Electronics Security Group* 8.

Fedrecheski, Geovane, Jan M. Rabaey, Laisa CP. Costa, Pablo C. Calcina Ccori, William T. Pereira ja Marcelo K Zuffo. 2020. “Self-sovereign identity for IoT environments: a perspective”. Teoksessa *2020 Global Internet of Things Summit (GIoTS),* 1–6. IEEE.

Ferdous, Md Sadek, Farida Chowdhury ja Madini O Alassafi. 2019. “In search of self-sovereign identity leveraging blockchain technology”. *IEEE Access* 7:103059–103079.

Foundation, Self Key. 2017. “Self-Sovereign Identity for more Freedom and Privacy—SelfKey”. *Selfkey.*

Guadagnoli, Edward, ja Wayne F. Velicer. 1988. “Relation of sample size to the stability of component patterns.” *Psychological bulletin* 103 (2): 265.

Jing, Y., J. Li, Y. Wang ja H. Li. 2021. “The Introduction of Digital Identity Evolution and the Industry of Decentralized Identity”, 504–508. Institute of Electrical / Electronics Engineers Inc. https://doi.org/10.1109/IAECST54258.2021.9695553.

Kangas, Petra. 2022. “Digitaalisen lompakon omaksumiseen vaikuttavat tekijät”. Pro gradu -tutkielma, Jyväskylän yliopisto.

Kim, Beomseok, Woonseob Shin, Dong-Yeop Hwang ja Ki-Hyung Kim. 2021. “Attribute-based access control (ABAC) with decentralized identifier in the Blockchain-based energy transaction platform”. Teoksessa *2021 International Conference on Information Networking (ICOIN),* 845–848. IEEE.

Kitchenham, Barbara, ja Stuart Charters. 2007. “Guidelines for performing systematic literature reviews in software engineering”.

Kuperberg, M., ja R. Klemens. 2022. “Integration of Self-Sovereign Identity into Conventional Software using Established IAM Protocols: A Survey”, 51–62. Gesellschaft fur Informatik (GI).

Laatikainen, Gabriella, Taija Kolehmainen ja Pekka Abrahamsson. 2021. “Self-sovereign identity ecosystems: benefits and challenges”. Teoksessa *Scandinavian Conference on Information Systems.* Association for Information Systems.

Lefever, Samuel, Michael Dal ja Ásrún Matthıasdóttir. 2007. “Online data collection in academic research: Advantages and limitations”. *British Journal of Educational Technology* 38 (4): 574–582.

Lesavre, Loic, Priam Varin, Peter Mell, Michael Davidson ja James Shook. 2019. “A taxonomic approach to understanding emerging blockchain identity management systems”. *arXiv preprint arXiv:1908.00929.*

Liu, Xing, Bahar Farahani ja Farshad Firouzi. 2020. “Distributed ledger technology”. Teoksessa *Intelligent Internet of Things,* 393–431. Springer.

Liu, Y., D. He, M.S. Obaidat, N. Kumar, M.K. Khan ja K.-K. Raymond Choo. 2020. “Blockchain-based identity management systems: A review”, https://doi.org/10.1016/j.jnca.2020.102731.

López, M. Allende. 2020. “Self-sovereign identity: The future of identity: Self-sovereignity, digital wallets, and blockchain”. *Inter-American Development Bank* 10:0002635.

Lundkvist, Christian, Rouven Heck, Joel Torstensson, Zac Mitton ja Michael Sena. 2016. *uPort: A platform for self-sovereign identity.* Tekninen raportti.

Metsämuuronen, Jari. 2011. *Tutkimuksen tekemisen perusteet ihmistieteissä : e-kirja opiskelijalaitos.* Painetun kirjan 2. ja 4. laitoksen pohjalta. Helsinki: International Methelp, Booky.fi. https://www.booky.fi/lainaa/1174.

Modinis, IDM. 2005. “Common terminological framework for interoperable electronic identity management”. *The 2005 Modinis IDM Study Team.*

Mühle, Alexander, Andreas Grüner, Tatiana Gayvoronskaya ja Christoph Meinel. 2018. “A survey on essential components of a self-sovereign identity”. *Computer Science Review* 30:80–86.

Naghmouchi, Montassar, Hella Kaffel Ben Ayed ja Maryline Laurent. 2022. “An automatized Identity and Access Management system for IoT combining Self-Sovereign Identity and smart contracts”. Teoksessa *Foundations and Practice of Security: 14th International Symposium, FPS 2021, Paris, France, December 7–10, 2021, Revised Selected Papers,* 208–217. Springer.

Naik, N., ja P. Jenkins. 2020a. “Governing principles of self-sovereign identity applied to blockchain enabled privacy preserving identity management systems”. Teoksessa *2020 IEEE International Symposium on Systems Engineering (ISSE),* 1–6. IEEE.

———. 2020b. “Self-Sovereign Identity Specifications: Govern your identity through your digital wallet using blockchain technology”. Teoksessa *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud),* 90–95. IEEE.

———. 2020c. “Your Identity is Yours: Take Back Control of Your Identity Using GDPR Compatible Self-Sovereign Identity”. Institute of Electrical / Electronics Engineers Inc. https://doi.org/10.1109/BESC51023.2020.9348298.

Naik, N., ja P. Jenkins. 2020d. “Your identity is yours: Take back control of your identity using GDPR compatible self-sovereign identity”. Teoksessa *2020 7th International Conference on Behavioural and Social Computing (BESC),* 1–6. IEEE.

Neuman, W. Lawrence. 2014. “Survey research”. Teoksessa *Social Research Methods: Qualitative and Quantitative Approaches,* 316–338. Pearson.

Nokhbeh Zaeem, Razieh, Kai Chih Chang, Teng-Chieh Huang, David Liau, Wenting Song, Aditya Tyagi, Manah Khalil, Michael Lamison, Siddharth Pandey ja K Suzanne Barber. 2021. “Blockchain-Based Self-Sovereign Identity: Survey, Requirements, Use-Cases, and Comparative Study”. Teoksessa *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology,* 128–135.

Petersen, Kai, Robert Feldt, Shahid Mujtaba ja Michael Mattsson. 2008. “Systematic mapping studies in software engineering”. Teoksessa *12th International Conference on Evaluation and Assessment in Software Engineering (EASE) 12,* 1–10.

Pfitzmann, Andreas, ja Marit Hansen. 2010. *A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management.*

Podsakoff, Philip M., Scott B. MacKenzie, Jeong-Yeon Lee ja Nathan P. Podsakoff. 2003. “Common method biases in behavioral research: a critical review of the literature and recommended remedies.” *Journal of applied psychology* 88 (5): 879.

Pöhn, D., M. Grabatin ja W. Hommel. 2021. “Eid and self-sovereign identity usage: An overview”, https://doi.org/10.3390/electronics10222811.

Pöhn, Daniela, Michael Grabatin ja Wolfgang Hommel. 2021. “eID and Self-Sovereign Identity Usage: An Overview”. *Electronics* 10 (22): 2811.

Rathore, Hem Shweta. 2016. “Adoption of digital wallet by consumers”. *BVIMSR’s journal of management research* 8 (1): 69.

Richter, Daniel, ja Jürgen Anke. 2021. “Exploring Potential Impacts of Self-Sovereign Identity on Smart Service Systems: An Analysis of Electric Vehicle Charging Services”. Teoksessa *Business Information Systems,* 105–116.

Saidi, H., N. Labraoui, A.A.A. Ari, L.A. Maglaras ja J.H.M. Emati. 2022. “DSMAC: Privacy-Aware Decentralized Self-Management of Data Access Control Based on Blockchain for Health Data”, 101011–101028. https://doi.org/10.1109/ACCESS.2022.3207803.

Satybaldy, Abylay, Anton Hasselgren ja Mariusz Nowostawski. 2022. “Decentralized Identity Management for E-Health Applications: State-of-the-Art and Guidance for Future Work”. *Blockchain in Healthcare Today* 5 (Special Issue).

Schardong, Frederico, ja Ricardo Custódio. 2022. “Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy”. *Sensors* 22 (15): 5641.

Shuaib, M., N.H. Hassan, S. Usman, S. Alam, S. Bhatia, P. Agarwal ja S.M. Idrees. 2022. “Land Registry Framework Based on Self-Sovereign Identity (SSI) for Environmental Sustainability”, https://doi.org/10.3390/su14095400.

Shuaib, M., N.H. Hassan, S. Usman, S. Alam, S. Bhatia, A. Mashat, A. Kumar ja M. Kumar. 2022. “Self-Sovereign Identity Solution for Blockchain-Based Land Registry System: A Comparison”, https://doi.org/10.1155/2022/8930472.

Siqueira, Alexandre, Arlindo Flavio Da Conceição ja Vladimir Rocha. 2021. “Blockchains and self-sovereign identities applied to healthcare solutions: A systematic review”. *arXiv preprint arXiv:2104.12298.*

Soltani, R., U.T. Nguyen ja A. An. 2021. “A Survey of Self-Sovereign Identity Ecosystem”, https://doi.org/10.1155/2021/8873429.

Song, Lihua, Mengchen Li, Zongke Zhu, Peng Yuan ja Yunhua He. 2020. “Attribute-based access control using smart contracts for the internet of things”. *Procedia computer science* 174:231–242.

Sporny, M., D. Longley, M. Sabadello, D. Reed, O. Steele ja C. Allen. 2022. “Decentralized Identifiers (DIDs) v1. 0 Core architecture, data model, and representations”. Viitattu 13. joulukuuta 2022. https://www.w3.org/TR/did-core/.

Sporny, M., G. Noble ja D. Longley. 2022. “Verifiable credentials data model v1. 1, 2022, Accessed: 2022-03-23”. Viitattu 13. joulukuuta 2022. https://www.w3.org/TR/vc-data-model/.

Stokkink, Quinten, ja Johan Pouwelse. 2018. “Deployment of a blockchain-based self-sovereign identity”. Teoksessa *2018 IEEE international conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData),* 1336–1342. IEEE.

Sunyaev, Ali. 2020. “Distributed ledger technology”. Teoksessa *Internet Computing,* 265–299. Springer.

Tobin, Andrew, ja Drummond Reed. 2016. “The inevitable rise of self-sovereign identity”. *The Sovrin Foundation* 29 (2016): 18.

Wang, Fennie, ja Primavera De Filippi. 2020. “Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion”. *Frontiers in Blockchain,* 28.

Vilkka, Hanna. 2007. *Tutki ja mittaa: Määrällisen tutkimuksen perusteet.*

Windley, P., ja Reed D. Sovrin. 2018. “A Protocol and Token for Self-Sovereign Identity and Decentralized Trust”. *Utah: Sovrin Foundation.*

Yang, Xiaohui, ja Wenjie Li. 2020. “A zero-knowledge-proof-based digital identity management scheme in blockchain”. *Computers & Security* 99:102050.

Yong, An Gie, Sean Pearce ym. 2013. “A beginner’s guide to factor analysis: Focusing on exploratory factor analysis”. *Tutorials in quantitative methods for psychology* 9 (2): 79–94.

Liitteet

A Kyselylomake

Itsehallittavan identiteetin koetut hyödyt ja haasteet

☐ Pakolliset kysymykset merkitty tähdellä (*)

Hei, tämä kysely on osa Jyväskylän yliopistossa toteutettavaa tietojärjestelmätieteiden ja tietotekniikan pro gradu -tutkielmaa, jossa tarkastelemme itsehallittavan identiteetin potentiaalisia hyötyjä ja haasteita. Tavoitteenamme on kartoittaa mahdollisten loppukäyttäjien näkemyksiä itsehallittavaan identiteettiin liittyvistä hyödyistä ja haasteista Suomen uuden digitaalisen henkilöllisyystodistuksen valossa.

Kyselyn arvioitu kesto on 5-10 minuuttia. Vastaukset ovat anonyymejä, eikä yksittäistä vastaaja voida tunnistaa. Tuloksia hyödynnetään ainoastaan tässä tutkimuksessa.

Kiitos osallistumisesta!

Tutustu tietosuojailmoitukseen: tietosuojailmoitus

Tutkijoiden yhteystiedot:
Ekku Sipilä, tietotekniikan maisteriopiskelija
ekku.s.sipila@student.jyu.fi

Mikael Ruotsalainen, tietojärjestelmätieteiden maisteriopiskelija
mikael.j.j.ruotsalainen@student.jyu.fi

Aihepiirin esittely

Itsehallittava identiteetti on uusi digitaalisen identiteetin muoto. Digitaalisella identiteetillä voidaan tarkoittaa mitä tahansa tunnuksia ja niihin linkitettävissä olevaa informaatiota. Esimerkiksi Google- tai Facebook-tunnus ja kaikki tunnukseen liittyvä informaatio muodostavat yhdessä digitaalisen identiteetin. Googlen ja Facebookin käyttäjien digitaaliset identiteetit eivät kuitenkaan ole itsehallittavia identiteettejä. Itsehallittavalla identiteetillä viitataan siihen, että käyttäjällä on täysi hallinta omasta digitaalisesta identiteetistään. Käytännössä tämä tarkoittaa sitä, että käyttäjä voi hallita itse, mitä tietoja hänestä tallennetaan ja miten tietoja käytetään.

Suomen Digi- ja tietoväestövirastolla on käynnissä hanke itsehallittavaan identiteettiin pohjautuvan uuden digitaalisen henkilöllisyystodistuksen kehittämiseksi. Käyttäjät hallitsevat ja käyttävät uutta henkilöllisyystodistusta älylaitteeseen asennettavassa Suomi.fi-lompakko-sovelluksessa. Hankkeessa kehitetään myös uusi tunnistautumistapa ajamaan nykyisen vahvan tunnistautumisen virkaa. Uuden henkilöllisyystodistuksen avulla voit siis tunnistautua asioidessasi esimerkiksi sairaalassa tai Alkossa, sekä kirjautua vahvan tunnistautumisen vaativiin järjestelmiin, kuten Omakantaan. Vanha henkilöllisyystodistus tulee säilymään kuitenkin uuden rinnalla.

Lisätietoa Suomen digitaalisen henkilöllisyystodistuksen uudistuksesta löydät halutessasi alta:
https://dvv.fi/digitaalisen-henkilollisyyden-uudistus

Taustatiedot

1. Ikä (vuosina) *

◯ Alle 18

- ◯ 18-30
- ◯ 31-40
- ◯ 41-50
- ◯ 51-60
- ◯ 61-70
- ◯ 71+

2. Koulutus *

- ◯ Peruskoulu
- ◯ Ylioppilas- tai ammatillinen tutkinto
- ◯ Alempi korkeakoulututkinto
- ◯ Ylempi korkeakoulututkinto
- ◯ Tohtorikoulutus
- ◯ Muu koulutus, mikä?

3. Pääasiallinen toimesi *

- ◯ Työssäkäyvä
- ◯ Yrittäjä
- ◯ Opiskelija
- ◯ Eläkeläinen
- ◯ Työtön
- ◯ Jokin muu, mikä?

4. Työala, mikäli olet töissä

- ◯ En ole töissä
- ◯ Kirjanpito, pankki- tai rahoitusala
- ◯ Liiketoiminta, konsultointi tai johtaminen
- ◯ Luovat taiteet tai muotoilu
- ◯ Energia- ja yleishyödylliset palvelut
- ◯ Insinöörityö tai valmistusteollisuus
- ◯ Terveydenhuolto
- ◯ Ympäristö tai maatalous
- ◯ Markkinointi, mainonta tai PR-toiminta
- ◯ Media
- ◯ Kiinteistöt tai rakentaminen
- ◯ Julkiset palvelut tai julkishallinto
- ◯ Rekrytointi tai HR
- ◯ Vähittäismyynti
- ◯ Lääketiede ja lääkevalmisteet
- ◯ Sosiaalihuolto

- ◯ Tapahtumien tai tilaisuuksien järjestäminen
- ◯ Tietojenkäsittely tai IT
- ◯ Oikeus ja laki
- ◯ Lainvalvonta ja turvallisuus
- ◯ Muu, mikä?
- ◯ Koulutusala
- ◯ Kuljetus tai logistiikka
- ◯ Hyväntekeväisyys- tai vapaaehtoistyö
- ◯ Vapaa-aika, urheilu tai matkailu

5. Miten pätevä koet olevasi IT-taidoissa? *

◯ Erittäin pätevä ◯ Pätevä ◯ Kohtalaisen pätevä ◯ En erityisen pätevä ◯ En lainkaan pätevä

6. Miten paljon tiedät ennestään itsehallittavasta identiteetistä tai Suomen uudesta digitaalisesta henkilöllisyystodistuksesta? *

◯ Paljon ◯ Jonkin verran ◯ Hieman ◯ Vähän ◯ En mitään

7. Miten todennäköisesti tulet ottamaan uuden digitaalisen henkilöllisyystodistuksen käyttöön? *

◯ Hyvin todennäköisesti ◯ Melko todennäköi-sesti ◯ En osaa sanoa ◯ Melko epätodennäköi-sesti ◯ Hyvin epätodennäköisesti

Alla oleva johdantoteksti esiteltiin jo kyselyn alussa, mutta voit tarvittaessa palata siihen tässä.

Itsehallittava identiteetti on uusi digitaalisen identiteetin muoto. Digitaalisella identiteetillä voidaan tarkoittaa mitä tahansa tunnuksia ja niihin linkitettävissä olevaa informaatiota. Esimerkiksi Google- tai Facebook-tunnus ja kaikki tunnukseen liittyvä informaatio muodostavat yhdessä digitaalisen identiteetin. Googlen ja Facebookin käyttäjien digitaaliset identiteetit eivät kuitenkaan ole itsehallittavia identiteettejä. Itsehallittavalla identiteetillä viitataan siihen, että käyttäjällä on täysi hallinta omasta digitaalisesta identiteetistään. Käytännössä tämä tarkoittaa sitä, että käyttäjä voi hallita itse, mitä tietoja hänestä tallennetaan ja miten tietoja käytetään.

Suomen Digi- ja tietoväestövirastolla on käynnissä hanke itsehallittavaan identiteettiin pohjautuvan uuden digitaalisen henkilöllisyystodistuksen kehittämiseksi. Käyttäjät hallitsevat ja käyttävät uutta henkilöllisyystodistusta älylaitteeseen asennettavassa Suomi.fi-lompakko-sovelluksessa. Hankkeessa kehitetään myös uusi tunnistautumistapa ajamaan nykyisen vahvan tunnistautumisen virkaa. Uuden henkilöllisyystodistuksen avulla voit siis tunnistautua asioidessasi esimerkiksi sairaalassa tai Alkossa, sekä kirjautua vahvan tunnistautumisen vaativiin järjestelmiin, kuten Omakantaan. Uuden henkilöllisyystodistuksen on tarkoitus tulla käyttöön syksyllä 2023. Vanha henkilöllisyystodistus tulee säilymään kuitenkin uuden rinnalla.

Lisätietoa Suomen digitaalisen henkilöllisyystodistuksen uudistuksesta löydät halutessasi alta:
https://dvv.fi/digitaalisen-henkilollisyyden-uudistus

Koetut hyödyt

8. Ilmoita, miten tärkeää seuraavien väittämien toteutuminen on sinulle uuden digitaalisen henkilöllisyystodistuksen osalta *

	Erittäin tärkeää	Tärkeää	Melko tärkeää	Ei erityisen tärkeää	Ei tärkeää
Minulla on mahdollisuus päättää itse, miten tietojani jaetaan ja käytetään *	○	○	○	○	○
Yksityisyyteni on paremmin turvattu *	○	○	○	○	○
Minulla on mahdollisuus jakaa vain minimimäärän tietoja itsestäni *	○	○	○	○	○
Tietojeni jakaminen ja käyttö on läpinäkyvää *	○	○	○	○	○
Henkilötietojeni tietoturva paranee *	○	○	○	○	○
Toimintani valvominen vähenee *	○	○	○	○	○
Tunnistautuminen on helppoa ja intuitiivista *	○	○	○	○	○
Voin käyttää samaa henkilöllisyystodistusta useissa järjestelmissä ja maissa *	○	○	○	○	○
Minun ei tarvitse kantaa erillistä fyysistä henkilöllisyystodistusta mukanani *	○	○	○	○	○
Kaikilla on mahdollisuus ottaa uusi henkilöllisyystodistus käyttöön *	○	○	○	○	○

9. Mitkä näet tärkeimpinä edellä esitetyistä hyödyistä? Ruksi kolme (3) kohtaa. *

- ☐ Minulla on mahdollisuus päättää itse, miten tietojani jaetaan ja käytetään
- ☐ Yksityisyyteni on paremmin turvattu
- ☐ Minulla on mahdollisuus jakaa vain minimimäärän tietoja itsestäni
- ☐ Tietojeni jakaminen ja käyttö on läpinäkyvää
- ☐ Henkilötietojeni tietoturva paranee
- ☐ Toimintani valvominen vähenee
- ☐ Tunnistautuminen on helppoa ja intuitiivista
- ☐ Voin käyttää samaa henkilöllisyystodistusta useissa järjestelmissä ja maissa
- ☐ Minun ei tarvitse kantaa erillistä fyysistä henkilöllisyystodistusta mukanani
- ☐ Kaikilla on mahdollisuus ottaa uusi henkilöllisyystodistus käyttöön

10. Onko jotain muuta, minkä toteutumisen tai huomioon ottamisen uudessa henkilöllisyystodistuksessa koet tärkeääksi?

Alla oleva johdantoteksti esiteltiin jo kyselyn alussa, mutta voit tarvittaessa palata siihen tässä.

Itsehallittava identiteetti on uusi digitaalisen identiteetin muoto. Digitaalisella identiteetillä voidaan tarkoittaa mitä tahansa tunnuksia ja niihin linkitettävissä olevaa informaatiota. Esimerkiksi Google- tai Facebook-tunnus ja kaikki tunnukseen liittyvä informaatio muodostavat yhdessä digitaalisen identiteetin. Googlen ja Facebookin käyttäjien digitaaliset identiteetit eivät kuitenkaan ole itsehallittavia identiteettejä. Itsehallittavalla identiteetillä viitataan siihen, että käyttäjällä on täysi hallinta omasta digitaalisesta identiteetistään. Käytännössä tämä tarkoittaa sitä, että käyttäjä voi hallita itse, mitä tietoja hänestä tallennetaan ja miten tietoja käytetään.

Suomen Digi- ja tietoväestövirastolla on käynnissä hanke itsehallittavaan identiteettiin pohjautuvan uuden digitaalisen henkilöllisyystodistuksen kehittämiseksi. Käyttäjät hallitsevat ja käyttävät uutta henkilöllisyystodistusta älylaitteeseen asennettavassa Suomi.fi-lompakko-sovelluksessa. Hankkeessa kehitetään myös uusi tunnistautumistapa ajamaan nykyisen vahvan tunnistautumisen virkaa. Uuden henkilöllisyystodistuksen avulla voit siis tunnistautua asioidessasi esimerkiksi sairaalassa tai Alkossa, sekä kirjautua vahvan tunnistautumisen vaativiin järjestelmiin, kuten Omakantaan. Uuden henkilöllisyystodistuksen on tarkoitus tulla käyttöön syksyllä 2023. Vanha henkilöllisyystodistus tulee säilymään kuitenkin uuden rinnalla.

Lisätietoa Suomen digitaalisen henkilöllisyystodistuksen uudistuksesta löydät halutessasi alta:
https://dvv.fi/digitaalisen-henkilollisyyden-uudistus

Koetut haasteet

11. Ilmoita, missä määrin olet samaa mieltä seuraavista väittämistä uuden digitaalisen henkilöllisyystodistuksen suhteen.

Olen huolissani/koen haasteelliseksi että,... *

	Täysin samaa mieltä	Samaa mieltä	En samaa enkä eri mieltä	Eri mieltä	Täysin eri mieltä
...digitaalinen henkilöllisyystodistus vaatii älylaitteen toimiakseen *	○	○	○	○	○
...tunnusten palautus uudessa digitaalisessa henkilöllisyydessä voi olla vaikeaa, mikäli käyttäjä hukkaa tunnuksensa tai unohtaa salasanansa *	○	○	○	○	○
...uuden henkilöllisyystodistuksen käyttö voi lisätä epäoikeudenmukaisuutta, sillä kaikilla ei välttämättä ole tarvittavia laitteita tai kykenevyyttä sen käyttöön *	○	○	○	○	○

	Täysin samaa mieltä	Samaa mieltä	En samaa enkä eri mieltä	Eri mieltä	Täysin eri mieltä
..Suomen digitaalisessa henkilöllisyystodistuksessa käytetyt teknologiat ovat uusia, eikä niitä ole vielä tutkittu kattavasti *	○	○	○	○	○
...joillain käyttäjillä voi olla vaikeuksia uuden henkilöllisyystodistuksen hallintaan tarkoitetun sovelluksen käytössä *	○	○	○	○	○
...puhelimeni joutuessa vääriin käsiin, myös henkilöllisyystodistukseni vaarantuu *	○	○	○	○	○
...uusi henkilöllisyystodistus voi tuoda mukanaan uusia tietoturvariskejä, joita ei vanhojen menetelmien kanssa ilmennyt *	○	○	○	○	○
...uuden henkilöllisyystodistuksen väärinkäytön tai varkauden selvittäminen voi olla haastavaa, sillä henkilöllisyystodistuksen käytöstä ei tallennu tietoa *	○	○	○	○	○

12. Mitkä näet suurimpina edellä esitetyistä haasteista? Ruksi korkeintaan kolme kohtaa

- ☐ Digitaalinen henkilöllisyystodistus vaatii älylaitteen toimiakseen
- ☐ Tunnusten palautus uudessa digitaalisessa henkilöllisyydessä voi olla vaikeaa, mikäli käyttäjä hukkaa tunnuksensa tai unohtaa salasanansa
- ☐ Uuden henkilöllisyystodistuksen käyttö voi lisätä epäoikeudenmukaisuutta, sillä kaikilla ei välttämättä ole tarvittavia laitteita tai kykenevyyttä sen käyttöön
- ☐ Suomen digitaalisessa henkilöllisyystodistuksessa käytetyt teknologiat ovat uusia, eikä niitä ole vielä tutkittu kattavasti
- ☐ Joillain käyttäjillä voi olla vaikeuksia uuden henkilöllisyystodistuksen hallintaan tarkoitetun sovelluksen käytössä
- ☐ Puhelimeni joutuessa vääriin käsiin, myös henkilöllisyystodistukseni vaarantuu
- ☐ Uusi henkilöllisyystodistus voi tuoda mukanaan uusia tietoturvariskejä, joita ei vanhojen menetelmien kanssa ilmennyt
- ☐ Uuden henkilöllisyystodistuksen väärinkäytön tai varkauden selvittäminen voi olla haastavaa, sillä henkilöllisyystodistuksen käytöstä ei tallennu tietoa

13. Onko jotain muuta, minkä koet haasteelliseksi tai mistä olet huolissasi uuden henkilöllisyystodistuksen suhteen?

Kysely on nyt päättynyt. Lähetä vastaukset "Lähetä"-painikkeesta.

Kiitos kyselyyn osallistumisesta!

B Kirjallisuuskartoitus: hakulausekkeen kehitys

Hakusanat	Päivämäärä	Tietokanta	Osumat	Vuosi
“digital identity” AND (“self-sovereign” OR “ssi”)	30.9.2022	Scopus	107	
“digital identity” AND (“self-sovereign” OR “ssi”)	30.9.2022	Scopus	107	2018->
“digital identity” AND (“self-sovereign” OR “ssi”)	30.9.2022	Google Scholar	2060	
“digital identity” AND (“self-sovereign” OR “ssi”)	30.9.2022	Google Scholar	2010	2010->
“digital identity” AND (“self-sovereign” OR “ssi” OR “distributed ledger”)	5.10.2022	Scopus	143	
“digital identity” AND (“self-sovereign” OR “ssi” OR “blockchain”)	5.10.2022	Scopus	305	
“digital identity” AND (“self-sovereign” OR “ssi” OR “decentralized”)	5.10.2022	Scopus	188	
“digital identity” AND “decentralized”	5.10.2022	Scopus	130	
“digital identity” AND “distributed ledger”	5.10.2022	Scopus	64	
“digital identity” AND “blockchain”	5.10.2022	Scopus	274	
“self-sovereign” AND NOT “digital identity”	5.10.2022	Scopus	218	
“self-sovereign identity” AND NOT “digital identity”	5.10.2022	Scopus	172	
“digital identity” AND (“self-sovereign” OR “decentralized” OR “blockchain” OR “distributed ledger”)	5.10.2022	Scopus	188	

(“digital identity” AND (“self-sovereign” OR “decentralized” OR “blockchain” OR “distributed ledger”)) OR (“self-sovereign” AND NOT “digital identity”)	5.10.2022	Scopus	188	
“decentralized identity” OR “self-sovereign identity” OR “distributed identity”	12.10.2022	Scopus	478	
“decentralized identity” OR “self-sovereign identity” OR “distributed identity”	17.10.2022	Scoups	408	2018->

C Kirjallisuuskartoituksen tulokset: potentiaaliset hyödyt

Hyöty	Määrä
Yksityisyys (yht.)	62
Käyttäjällä on täysi kontrolli omasta identiteetistään	23
Yksityisyyden turva (privacy)	21
Datan minimalisointi (data minimalization)	6
Keskitetyn hallinnoinnin eliminointi/decentralization	6
Läpinäkyvyys (transparency)	5
Oikeus tulla unohdetuksi	1
Turvallisuus (yht.)	40
Tietoturva (data protection/security)	20
Datan pysyvyys (data permanence)	6
Luotettavuus	5
Yhden virhepisteen elimoininti (single point-of-failure)	4
Petosten havaitseminen	2
Datan muuttumattomuus (immutability)	2
Valvonnan väheneminen	1
Käytettävyys(yht.)	32
Parantaa yleisesti käyttäjäkokemusta	8
Siirrettävyys (portability)	8
Yhteentoimivuus (interoperability)	5
Automaattinen auktorisointi (auto authorization)	3
Ajan säästäminen	3
Automaattinen autentikointi (auto authentication)	2
Tunnusten hallinnan helpottaminen	1
Ei tarvitse kantaa mukana fyysistä identiteettitodistusta	1
Poistaa/kehittää vanhoja ongelmallisia toimintamalleja	1
Resurssien säästäminen (yht.)	8
Resurssien säästäminen/tehokkuus organisaatioille (esim. kulut)	4
Asiakkaan sisäänottoprosessin parantaminen ja tehostaminen	2
Työnkulun automatisointi (automated workflow)	1

Prosessien yksinkertaistaminen	1
Sekalainen (yht.)	8
Saatavuus	4
Käyttö ei vaadi paljoa suorituskykyä/muistia (IoT)	1
Käyttäjillä mahdollista saada palkkio datan jakamisesta	1
Standardien olemassaolo	1
Voisi hidastaa COVID-tartuntojen leviämistä	1

D Kirjallisuuskartoituksen tulokset: potentiaaliset haasteet

Haaste	Määrä
Tekniset haasteet (yht.)	33
Tunnusten (avaimen) palautus	18
Skaalautuvuus	4
Varastoinnin rajoitteet	3
Internetin tai muiden tarvittavien laitteiden puuttuminen	2
Transaktion validointiaika (lohkoketjut)	1
“ID Squatting” -ongelma	1
Vaatimus lohkoketjun käyttämiselle toteutuksessa	1
Offline käytön vaikeus	1
Käyttö vaatii spesifejä toiminnallisuuksia (IoT)	1
Nykyiset lohkoketjun toiminallisuudet/ominaisuudet eivät ole optimaalisia SSI:lle	1
Kehityksen ja standardien puute (yht.)	29
Standardien ja yhteisymmärryksen puute	14
Kehityksen ja tutkimuksen puute	7
Teknologiaosaamisen puute	4
SSI:n laajamittaisen käytön puute	3
Attribuuttien yhteensopivuus eri SSI-toteutuksien välillä (globaalin SSI:n kontekstissa)	1
Turvallisuuden ja yksityisyyden haasteet (yht.)	18
Digitaalisen lompakon joutuminen vääriin käsiin	5
Suljetun DLT:n -ongelmat	3
Vastuuvelvollisuuden määrittäminen (unlinkability/accountability)	3
Avoimen DLT:n -ongelmat	2
Sybil-hyökkäykset	1
“Key rotation” -ongelma	1
Altis DDoS-hyökkäyksille	1
Omien tunnuksien myyminen ja jakaminen on mahdollista	1

Jäljitettävyys (traceability)	1
Luottamuksen haasteet (yht.)	17
“Luottamusankkurin” puute	11
Datan eheys	3
Luottamuksen puute hallitusta kohtaan	2
Vaikeus saavuttaa korkean tason LoA	1
Sekalaiset haasteet (yht.)	15
Lailliset haasteet (esim. GDPR, eIDAS)	7
Saatavuus ja neutraalisuus	6
Kontrollin lisääntyminen	2
Kulujen nousu (yht.)	13
Vaatii suuria muutoksia organisaatioissa ja infrastruktuureissa	10
Kehityksen ja ylläpidon kustannukset	2
Lohkoketjun transaktioiden validoinnin kustannukset	1
Käytettävyyden haasteet (yht.)	9
Käyttäjäystävällisyys	6
Uupumus suostumuksen antamisesta	2
Vaikeus tehdä muutoksia käyttäjän tietoihin	1
Muutosvastahakoisuus (yht.)	8
Vastahakoisuus muutoksille	4
Hallituksen vastaisuus itsehallittavuutta kohtaan	2
Miten todistetaan, että SSI on kannattavaa liiketoiminnallisesti	2