Jatkuvan oppimisen identiteetinhallinta

Selvitys
11.2.2019

Manne Miettinen, Harri Honko, Jukka Kohtanen

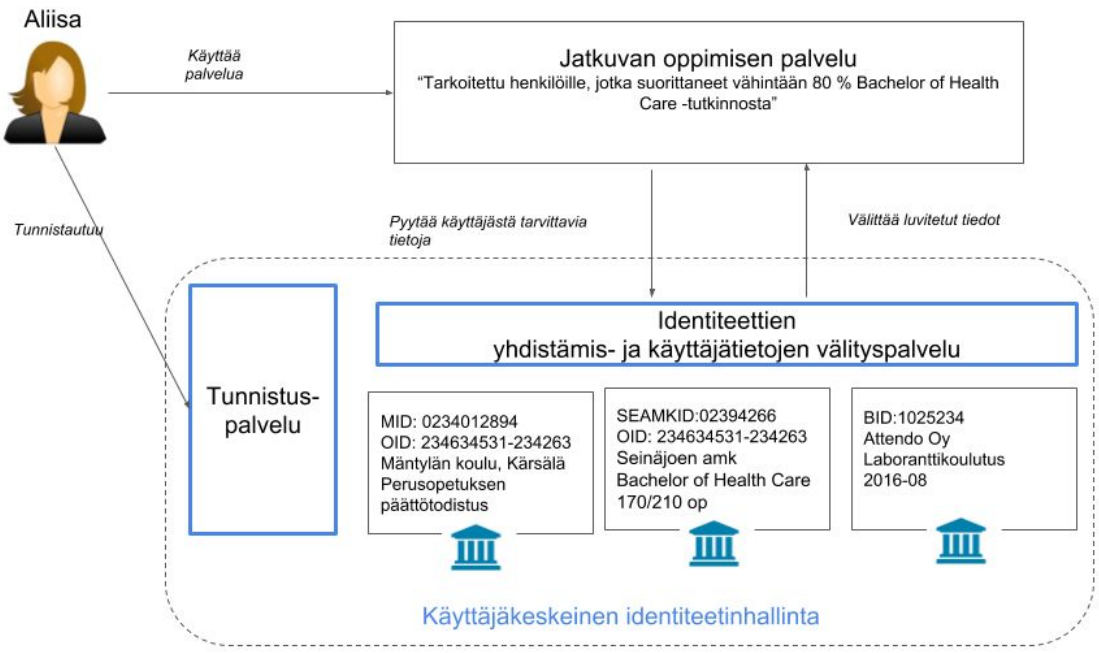
Sisällysluettelo

1 Tiivistelmä

Koulutuksen ja osaamisen merkitys työlle ja tuottavuudelle korostuu tulevaisuudessa sitä mukaa kun yhä enemmän perinteisiä asiantuntijatehtäviä voidaan automatisoida tai merkittävästi nopeuttaa koneoppimisen ja muun tietotekniikan avulla. Monivuotisen yhdessä oppilaitoksessa suoritettavan tutkinnon lisäksi tarvitaan nopeampia ja joustavampia keinoja päivittää kansalaisten osaamista.

Tässä selvityksessä tarkastellaan jatkuvan oppimisen tukemista tietotekniikan näkökulmasta. Etsimme vastausta siihen millainen tietotekninen infrastruktuuri tukisi parhaiten jatkuvan oppimisen edellyttämää joustavaa liikkumista erilaisten koulutusta tarjoavien organisaatioiden välillä.

Tällä hetkellä oppijoiden ja opettajien käyttäjätietojen hallinta perustuu oppilaitosten ylläpitämiin rekistereihin. Nykyjärjestelmä ei ole “rikki”, mutta on järkevä varautua jatkuvan oppimisen mahdollistamiseen hyvissä ajoin. Ehdotamme selvityksessä, että ratkaisua haettaisiin käyttäjäkeskeisen identiteetinhallinnan mallista. Tässä mallissa käyttäjä itse voisi hallinnoida osaa itseään koskevista tiedoista, joita eri koulutusorganisaatiot ovat hänestä kirjanneet.



Kuva 1. Käyttäjäkeskeinen identiteetinhallinta.

Karkeasti ottaen käyttäjäkeskeinen identiteetinhallinnan malli edellyttäisi, että käyttäjä voisi luoda itselleen pitkäaikaisen sähköisen identiteetin, johon hän voisi kytkeä muita sähköisiä identiteettejään. Yllä olevassa kuvassa Tunnistuspalvelu on palvelu, johon Aliisa on luonut itselleen pitkäikäisen sähköisen identiteetin, ja johon Aliisa voi tunnistautua sähköisesti (esimerkiksi näyttämällä sormenjälkeään älylaitesovellukselle). Identiteettien yhdistämis- ja käyttäjätietojen välityspalvelu on palvelu, jonka avulla Aliisa on yhdistänyt pitkäikäiseen identiteettiinsä kolmessa eri koulutusorganisaatiossa itsestään kirjatut tiedot.

2 Johdanto

2.1 Jatkuva oppiminen

Opetus- ja kulttuuriministeriön asettaman osaamisen tulevaisuuspaneelin kannanotossa Jatkuvan oppimisen Suomi todetaan, että maailmanlaajuisesti käynnissä oleva, pääosin automatisaation ja koneoppimisen aiheuttama, työn murros aiheuttaa suuren muutospaineen Suomen koulutusjärjestelmälle: “Uudenlainen työ vaatii uudenlaista osaamista. Sen takia käynnissä oleva työn murros on suuri haaste suomalaiselle osaamiselle. Perinteinen polku opinnoista työelämään ja lopulta eläkkeelle on rapistumassa ja sen tilalle on noussut ajatus jatkuvasta oppimisesta ja aktiivisesta osallistumisesta läpi koko elämän. Suomalainen koulutusjärjestelmä kaipaa päivitystä. Osaamisen turvaamiseksi on toteutettava laajamittainen jatkuvan oppimisen reformi. Sen myötä suomalaiset voivat kouluttautua tai kehittää osaamistaan joustavasti elämän aikana. Käytännössä reformi tarkoittaisi koko koulutusjärjestelmän tarjonnan joustavuuden merkittävää lisäämistä. Ihmisten tulisi päästä käsiksi tarvitsemaansa koulutukseen selvästi nykyistä helpommin myös työn ohessa ja sen aikana. Osaamisen kehittämisen puitteita kuten verotusta, sosiaaliturvaa ja erilaisia etuuksia olisi myös järjestelmällisesti kehitettävä jatkuvan oppimisen mahdollistamiseksi.”

Jatkuvan oppimisen aiheuttamat muutospaineet, ja vastaavasti toimenpiteet, joilla niihin pyritään vastaamaan, koskevat ennen kaikkea perusopetuksen jälkeistä aikaa. Perusopetuksen jälkeinen oppiminen korostuu helposti jatkuvaa oppimista koskevassa keskustelussa, mutta perusopetusta ja sitä edeltävää varhaiskasvatusta ei kuitenkaan tule missään nimessä unohtaa jatkuvan oppimisen pohdinnoista. Oppijan polulle lähdetään perusopetuslain (628/1998) velvoittamana. Oppivelvollisuus alkaa sinä vuonna kun lapsi täyttää seitsemän vuotta ja päättyy sen lukuvuoden lopussa sinä kalenterivuonna, jona nuori täyttää 17 vuotta. Käytännössä kaikki lapset (99,7 %) suorittavat perusopetuksen oppimäärän. Työn murroksen näkökulmasta perusopetuksen oppimäärä on välttämätön peruslähtökohta myöhemmälle oppimiselle.

Oppimisen tarkastelu tutkinto-opiskelupainotteisesta kertaluonteisesta projektista onkin yhä enemmän siirtymässä eliniän kestävään sykliin, jossa uutta opitaan ja hyödynnetään jatkuvasti. Perusta tälle luodaan lapsena ja oppiminen kasvaa kumulatiivisesti ja luo kullekin henkilölle uniikin osaamiskokonaisuuden, jota ruokitaan koko elinikä. Tutkintoon valmistuminen on vain yksi askel tätä prosessia. Jatkuvan oppimisen tukeminen ei koske vain koulutusta tai opiskelemista vaan se luo uudenlaisia vaatimuksia myös oppimista tukevalle infrastruktuurille ja palveluille. Oppiminen ei ole enää sidottu tiettyyn organisaatioon vaan sen tulee seurata oppijaa niiden tarpeiden mukaan, jotka osaamisen kehittäminen vaatii.

Jatkuvan oppimisen maailmassa oppijan polku kulkee useiden organisaatioiden ja toimijoiden läpi ja polun varrella tiedon täytyy seurata oppijaa. Myös tältä osin täytyy ajattelussa siirtyä oppijalähtöisyyteen ja purkaa järjestelemien ja palveluiden välisiä raja-aitoja ja täten poistaa

oppimisen esteitä. Toisaalta täytyy huomioida, että samalla henkilöstä jää tietoja eri toimijoiden rekistereihin ja tietokantoihin — tietoja, jotka täytyy suojata mutta jotka myös täytyy olla tarvittaessa käytettävissä. Tähän päästään vain sillä, että monimutkaiset, eri toimijoista koostuvat verkostot toimivat tehokkaasti yhdessä. Yksi osa käytännön toteutusta tulee olla tietojärjestelmien yhteentoimivuus. Tässä selvityksessä tarkastellaan lähemmin tietojärjestelmien yhteentoimivuuden yhtä osa-aluetta, identiteetinhallintaa.

2.2 Identiteetinhallinnan peruskäsitteet

Ennen tarkempaa pureutumista haasteisiin, joita jatkuvan oppimisen mahdollistaminen aiheuttaa identiteetinhallinnalle, on tarpeen määritellä eräitä jatkossa käytettäviä keskeisiä peruskäsitteitä.

Identiteetinhallinnalla tarkoitetaan prosessia, jolla käyttäjän esim. oppijan tietoja ylläpidetään tietojärjestelmissä. Identiteetinhallinta ei ole vain tietotekniikkaa, vaan myös määrämuotoisia toimintatapoja ja tietomalleja, jotka sovitaan tiedon hyödyntäjien kesken[1]. Mitä tietoja eri tahot tarvitsevat oppijoista? Mikä on minkäkin tiedon perustietolähde? Miten nämä tiedot määritellään, niin että ne ovat eri toimijoiden kesken yhteismitallisia? Miten varmistetaan, että tietoja voivat käsitellä vain ne, joilla on siihen oikeus?

Sähköisellä identiteetillä tarkoitetaan henkilöä koskevien tietojen kokoelmaa tietojärjestelmässä. Minimissään sähköinen identiteetti on yksilöintitunnus, jolla käyttäjä erotetaan toisista järjestelmän käyttäjistä. Laajempaan sähköiseen identiteettiin kuuluu käyttäjiä kuvaavia tietoja, **(käyttäjä)attribuutteja.** Sähköisestä identiteetistä puhuttaessa on tarpeen erottaa käsitteet henkilöllisyys ja sähköinen identiteetti. Henkilöllä (identiteetin tai identiteettien omistajalla) on vain yksi henkilöllisyys, mutta hänellä voi olla useita sähköisiä identiteettejä, esimerkiksi Ervi Esimerkillä voi olla seitsemän sähköistä identiteettiä: Helsingin kaupungin Wilmassa, Väestötietojärjestelmässä, Googlen pilvipalvelussa, Opintopolussa, Instagramissa ja Facebookissa.

Sähköinen tunnistaminen (sähköinen autentikointi eli **identiteetin todentaminen)** on menetelmä, jolla tietojärjestelmä varmistaa, että sähköinen identiteetti todella kuuluu sen omistajalle. Tunnistaminen voi perustua johonkin, 1) mitä käyttäjä tietää tai muistaa (esimerkiksi salasana), 2) jotain mitä käyttäjällä on hallussaan (esimerkiksi varmennekortti) tai 3) jotain mitä käyttäjä on (esimerkiksi sormenjälki tai muu biometrinen tunniste). Tunnistuksen varmuutta voi nostaa yhdistämällä edellä lueteltuja ns. tunnistustekijöitä, esimerkiksi varmistamalla ensin, että käyttäjällä on hallussaan varmennekortti ja sen lisäksi varmistamalla, että käyttäjä tietää korttiinsa liittyvän PIN-koodin. On syytä tiedostaa, että sähköisen identiteetin **varmuus** (Level of

[1] Linden, M. (2015). Identiteetin- ja pääsynhallinta. Tampere University of Technology. Department of Pervasive Computing. Report; Vuosikerta 6. Tampere University of Technology. https://tutcris.tut.fi/portal/files/3087873/linden_identiteetin_ja_paasynhallinta.pdf

Assurance, LOA) nähdään tunnistuksen varmuutta laajempana, useasta tekijästä koostuvana kokonaisuutena (esim. REFEDS Assurance Framework, NIST-800-63 ja RFC 8485).
Käyttäjä on luonnollinen henkilö ja sähköisen identiteetin omistaja, joka käyttää sähköistä asiointipalvelua. Jatkuvan oppimisen kontekstissa käyttäjä on esimerkiksi opiskelija, joka käyttää sähköistä asiointipalvelua kurssi-ilmoittautumiseen, kurssin suorittamiseen, tutkimusaineiston analysoimiseen tmv). Käyttäjällä voi olla (usein väliaikainen) sidos työnantajaan, oppilaitokseen, opiskelutilaan tmv. joka liittyy sähköisen asiointipalvelun käyttöön.

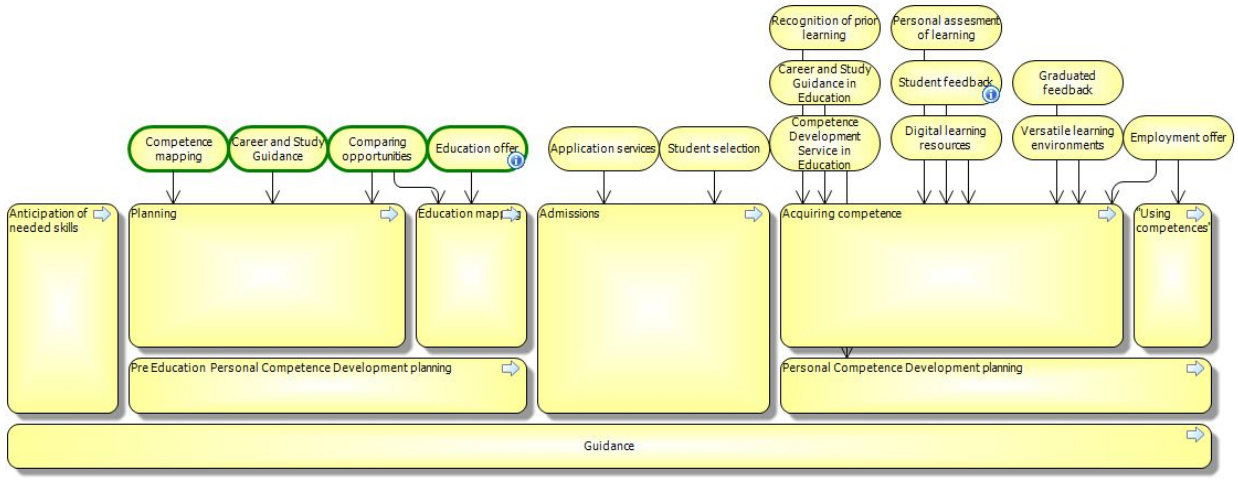
Sähköinen asiointipalvelu (tai lyhyesti **palvelu)** on digitaalinen aineeton hyödyke, joka tuottaa käyttäjälle jotain hyötyä. Palvelun tarjoava organisaatio kantaa tunnistamiseen liittyvän riskin, joten sen vastuulla määritellä mitä käyttäjätietoja se tarvitsee ja kuinka varma tunnistus on riittävä. Yksinkertaisimmillaan palvelun ei tarvitse tunnistaa käyttäjää lainkaan, vaan palvelu on kaikille käyttäjille sama. Kehittyneemmät palvelut tarjoavat erilaisia toimintoja erilaisille käyttäjille, jota varten palvelu tarvitsee käyttäjästä tietoja pystyäkseen päättämään millainen käyttäjä on kyseessä.

Identiteetin omistaja (engl. identity owner) on luonnollinen henkilö, jota sähköiseen identiteettiin liitetyt tiedot kuvailevat, ja joka käyttää palveluntarjoajan kautta tarjolla olevaa identiteettiä. Kun identiteetin omistaja antaa jollekin rekisterinpitäjälle pääsyn omiin henkilötietoihinsa, tulee hänestä yleisessä tietosuoja-asetuksessa tarkoitettu **rekisteröity** (engl. data subject).

Tunniste (yksilöintitunnus) on identiteetin omistajan rekisterinpitäjälle jakama, väitteisiin yhdistetty tieto, jonka avulla rekisterinpitäjä tunnistaa (identifioi) rekisteröidyn (engl. identifier).

2.3 Jatkuvan oppimisen haasteet identiteetinhallinnalle

Tarkastellaan sitten tarkemmin millaisia haasteita jatkuva oppiminen aiheuttaa identiteetinhallinnalle. Alla olevassa kuvassa on esitetty jäsennys jatkuvan oppimisen polulla tarvittavista päätoimintaprosesseista ja niitä tukevista digitaalisista palveluista. Kuva on peräisin EU:n rahoittaman Compleap-hankkeen arkkitehtuuridokumentaatiosta, jonka tavoitteena on suunnitella oppijakeskeinen digitaalinen ekosysteemi jatkuvan oppimisen tarpeisiin. Jatkuvan oppimisen toimijoita ja rooleja on kuvattu myös Korkeakoulujen opiskelun ja opetuksen tukipalveluiden ja hallinnon (OPI) viitearkkitehtuurissa.



Kuva 2. Digitaalisen oppijan polku ja päätoimintaprosessit (Compleap)

Kuva keskittyy lakisääteisen perusopetuksen jälkeiseen oppijan polkuun, jossa oppija suunnittelee koulutuksen hankkimista (Planning ja Education mapping), hakeutuu koulutukseen ja vastaanottaa paikan (Admissions), suorittaa opintoja (Acquiring competencies) ja hyödyntää oppimaansa (Using competences). Opintojen suorittamisen palveluita käytetään kuitenkin yhä enenevässä määrin jo perusopetuksessa, joten sitä ei tule unohtaa identiteetinhallinnan haasteista.

Tunnistamisen ja attribuuttien tarpeet vaihtelevat polun eri vaiheissa. Lakisääteisen opetuksen jälkeisiä opintoja suunnittelevaa oppijaa ei ole aina välttämätöntä tunnistaa. Tunnistamisen tarve kasvaa vasta opiskelupaikan haku- ja vastaanottovaiheessa, jolloin oppija täytyy tunnistaa, jotta hänet voidaan lisätä opiskelijarekisteriin ja hänelle syntyy opiskeluoikeus. Opiskeluvaiheessa (acquiring competencies) oppijan tulee voida tunnistautua usean eri koulutusorganisaation palveluihin riippumatta koulutuksen järjestäjästä, koulutusasteesta ja jopa maasta huolimatta siitä, onko henkilö opiskelemassa, työelämässä tai muussa elämänvaiheessa; palveluiden tulee voida yhdistää oppija samaan käyttäjään, jolla on niiden kannalta tarpeellista tietoa toisissa palveluissa. Palveluiden kautta saatujen todistusten ja pätevyyksien tulee linkittyä sitovasti oppijan yksilöivään pitkäikäiseen tunnisteeseen riippumatta palvelussa käytetyistä paikallisista tunnuksista.

Osa jatkuvaan oppimiseen liittyvistä uusista palveluista tulee olemaan yksilöiden käytettävissä jo perusopetuksen aikana, ennen kuin heistä tulee opiskelijoita toisen tai korkea-asteen oppilaitoksissa. Toisaalta henkilö voi tarvita palveluita opiskeluajan jälkeen, jolloin tunnistuksen näkökulmasta syntyy tilanne missä yksilö on palveluiden piirissä jo ennen varsinaisen roolitiedon syntymistä. Palveluiden eri toiminnot voivat edellyttää eri vahvuista tunnistamista: osaa palveluista voi käyttää ilman tunnistamista (anonyymisti), osaa heikon tunnistuksen jälkeen (esimerkiksi oppimateriaalin lukuoikeus) ja joissakin tapauksissa vahvan tunnistuksen jälkeen, esimerkiksi kun otetaan vastaan opiskelupaikka korkeakoulussa. Opintojen

suorittamisen palveluita käytetään päivittäin, joten tunnistautumisen pitäisi tapahtua mahdollisimman automaattisesti ja käyttäjäystävällisesti. Perusopetuksessa käytettävät opetusvälineet ovat opetuksen järjestäjän tarjoamia ja oppilaalle maksuttomia. Tämä voi rajoittaa perusopetuksessa käytettäviä tunnistusmenetelmiä. Esimerkiksi oppilaan oman älypuhelimen edellyttäminen voi olla ongelmallista maksuttomuuden näkökulmasta.

Opintoihin hakeutumisvaiheeseen liittyy yksilön tieto- ja oikeussuojanäkökulma: hakijan nimi, ikä, sukupuoli, kuva, siviilisääty, jäsenyydet tmv. eivät saisi aiheuttaa hyväksymispäätöksen tekijöiden asenteisiin (bias). Suomeen syntymässä oleva uusi politiikkalohko, tietopolitiikka, pyrkii nostamaan julkiseen keskusteluun ja julkisen vallan säädeltäviksi juuri tällaiset tietojen hyödyntämisen eettiset kysymykset. Hallituksen 5.12.2018 hyväksymässä Tietopoliittisessa selonteossa yhdenvertaisuus, oikeudenmukaisuus ja muut ns. keskitason periaatteet nähdään eettisen tietopolitiikan keskeisenä sisältönä. Toisaalta myöhemmin anonyymin hakijan pätevyydet ja identiteetti on itse päätösprosessissa (opiskelupaikan vastaanottaminen) pystyttävä varmentamaan. Tarve erilaisiin käyttäjään liittyviin tietoihin samoin kuin tunnistautuminen ja sen vahvuus siis vaihtelevat tarpeen mukaan eri toiminnoissa.

2.4 Käyttäjäkeskeinen identiteetinhallinta ja sen käsitteistö

Opetuksen ja koulutuksen järjestäjät hallinnoivat yleensä opiskelijoiden ja henkilökuntansa sähköisiä identiteettejä keskitetysti ns. **identiteetinhallintajärjestelmällä** (IdM-järjestelmä), joka on tehokas tapa hallinnoida käyttäjätietoja organisaation sisällä. Identiteetinhallintajärjestelmän perusidea on tyypillisesti synkronoida sähköiseen identiteettiin liittyviä tietoja eri tietojärjestelmien välillä siten, että eri tiedoilla (esim. nimitieto) on päätietolähteensä, josta tieto kopioidaan kyseistä tietoa hyödyntäviin järjestelmiin, niin että vältetään eri versiot samasta tiedosta.

Valtakunnallisen ja kansainvälisen yhteistyön lisääntyessä identiteetinhallinnan tulee mahdollistaa joustava pääsy oppijaa koskeviin tietoihin eri palveluissa ja oppilaitoksissa. Tämä on haaste edellä kuvatulle IdM-järjestelmää hyödyntävälle **organisaation sisäiselle käyttäjähallinnnolle**. Yksi menestyksekäs tapa vastata tähän haasteeseen on ollut ns. **käyttäjähallinnon luottamusverkostot** (eli **identiteettifederaatiot**), jotka laajentavat organisaatiokeskeisen käyttäjähallinnon organisaatioiden väliseksi tai **organisaatiorajat ylittäväksi käyttäjähallinnoksi**. Luottamusverkostossa usean eri organisaation IdM-järjestelmät kytketään tunnistusrajapintaan, jonka kautta ne voivat välittää käyttäjätietoja toisille rajapintaan kytketyille luotetuille organisaatioille. Luottamusverkostossa organisaatiot siis sopivat luottavansa toistensa käyttäjätietoihin. Suomessa ja muualla Euroopassa ovat korkeakoulut jo yli kymmenen vuoden ajan olleet edelläkävijöitä luottamusverkostojen hyödyntämisessä. Korkeakouluopiskelijat ja tutkijat kirjautuvat opetuksen ja tutkimuksen palveluihin yli 30 miljoonaa kertaa vuodessa organisaatiorajat ylittäen Haka-luottamusverkoston kautta. Identiteettifederaation haasteeksi nousevat kuitenkin federaatiorajat ja käyttäjät, joilla ei ole selkeää kytköstä luottamusverkostoon kuuluvaan organisaatioon. Kansainvälisissä tutkijaverkostoissa syntyy helposti tilanne, että osa yhteistyön kannalta oleellisista yksilöistä tai organisaatioista ei ole identiteettifederaation piirissä, eivätkä voi siihen helposti liittyä federaation sopimuksiin kirjattujen sääntöjen tai muiden rajausten tähden.

EU-kansalaisten tunnistamiseen tarkoitettu **eIDAS**[2] (Electronic Identification, Authentication and Trust Services) on esimerkki toisenlaisesta identiteettifederaatiosta. Sen tarkoitus on mahdollistaa eri jäsenmaiden kansallisten vahvojen tunnistusvälineiden käyttö rajojen yli siten, että esimerkiksi suomalaiseen julkishallinnon palveluun voisi tunnistautua espanjalaisella sähköisellä henkilökortilla. Suomen eIDAS-solmupisteesta vastaa Väestörekisterikeskus, ja se on toteutettu suomi.fi-tunnistuksen yhteyteen.

Organisaatiokeskeisen identiteetinhallinnan ongelma ovat käyttäjät, jotka liittyvät organisaatioon epäsuorasti. Koulutustoimialalla tähän ryhmään kuuluvat esimerkiksi työpaikkaohjaajat ammatillisessa koulutuksessa, alaikäisten oppijoiden huoltajat sekä henkilökuntaan

[2] eIDAS-toteutus on määritetty asetuksessa 910/2014 siihen liittyvällä teknisellä eID-profiilimäärittelyllä ja täytäntöönpanoasetuksella 2015 / 1502 tunnistamisen luottamustasoista.

kuulumattomat työntekijät, joiden tarjoamat palvelut on hankittu esimerkiksi ostopalveluna. Jatkuvan oppimisen maailmassa tämä käyttäjäryhmä oletettavasti kasvaa. Organisaatiorajat ylittävä käyttäjähallinto ei itsessään ratkaise sitä, miten näiden **organisaatioon kuulumattomien** käyttäjäryhmien tunnistus ja valtuuttaminen järjestetään. Toinen tunnistukseen liittyvä ongelma on, miten eri käyttäjäryhmien tunnusten ylläpitoa ja elinkaarta kätevästi hallinnoidaan.

Yksi vaihtoehto lisätä jatkuvan oppimisen edellyttämää joustavuutta olisi muuttaa lähestymistapaa sähköiseen identiteettiin ja siirtyä **käyttäjäkeskeiseen identiteetinhallintaan**. Käyttäjäkeskeinen identiteetinhallinta voi olla joko **keskitetyn toimijan hallinnoimaa** tai täysin **itsehallittava** (engl. self-sovereign identity, SSI).

Käyttäjäkeskeisessä mallissa luonnollinen henkilö omistaa ja hallinnoi itse omia (tai huollettavansa) henkilötietojaan organisaatioiden tukemana. Keskitetyn toimijan hallinnointimallissa henkilötiedot kerätään itse hallinnoitavan tilin yhteyteen, mutta itse tiliä tarjoaa keskitetty operaattori. Täysin itsehallittavan identiteetin mallissa käyttäjä vastaa myös tilistään itse.

Itsehallittavassa mallissa henkilötiedot on talletettu jokaiselle käyttäjälle itselleen, joten yksittäistä vikaantumispistettä tai merkittävää hyökkäyskohdetta identiteettivarkauksille ei ole, toisin kuin keskitetyissä tietokannoissa. Paremmalla tietoturvalla on kuitenkin hintansa: itsehallittavan mallin hajautus on teknisesti monimutkaisempi ja siten kalliimpi toteuttaa. Vastuu tietojen tallennuksesta, turvakopioinnista ja tallennuslaitteiden ylläpidosta voi olla monelle käyttäjälle rasite itsehallittavassa mallissa

Sekä keskitetyn että itsehallitun käyttäjäkeskeisen identiteetinhallinnan malleissa käyttäjä ylläpitää itse häntä itseään koskevien tietojen rekisteriä, josta hän voi luovuttaa itseään koskevia tietoja. Tiedot tulevat käyttäjäkeskeisen identiteetin järjestelmään joko käyttäjältä itseltään tai joltakin luotettavalta oikeushenkilöltä, kuten valtiolta, organisaatiolta tai yrityksiltä. Tietojen luotettavuuden vuoksi käyttäjän itsensä lisäämät tiedot, eli väitteet, ovat yksinkertaisia, kuten sähköpostiosoite tai puhelinnumero. Kolmansilta tahoilta myönnetyt varmenteet luovat pohjan varmennettaville väitteille, joiden avulla tiedon vastaanottaja voi olla varma merkittävän henkilötiedon totuudenmukaisuudesta. Tällaisia tietoja voisivat Suomessa olla esimerkiksi Väestörekisterikeskuksen antama henkilötunnus, Opetushallituksen antama kansallinen oppijanumero, yliopiston myöntämä todistus koulutuksesta, yksityisen koulutustoimijan antama pätevyystodistus tai Liikenne- ja viestintäviraston antama tieto voimassaolevasta raskaan ajoneuvon ajo-oikeudesta. Viime kädessä väitteet ja niihin liittyvät tiedot on tallennettu käyttäjän hallinnoimaan joko keskitetyn operaattorin ylläpitämään rekisteriin tai itsehallittavassa mallissa käyttäjän omalla älylaitteella sijaitsevaan **identiteettilompakkoon** (engl. identity wallet), joka on suojattu vahvasti esimerkiksi sormenjälkitunnistuksella.

Henkilö voi asioida toisen puolesta siten, että valtuutustiedot tuodaan identiteettilompakkoon väitteenä “NN on tunnisteen Y virallinen edunvalvoja päivämäärään pv.kk.vvvv asti, myöntänyt/vahvistanut hetkellä T tunniste Y”.

Attribuuttitietoja yhdistelemällä tai rajaamalla voidaan luoda kulloinkin käyttötilanteessa tarpeellisia, mutta rajattuja henkilötietoja, eli **julkituonteja** (engl. proof). Julkituonnin luomista edeltää yleensä tunnistajan tunnistamistapahtuman alussa käyttäjän lompakolle toimittama pyyntö (engl. proof request). Edellä mainituilla **rajatuilla julkituonneilla** (engl. zero knowledge proof, ZKP) voidaan esittää kryptografisesti todennettavasti muun muassa tieto täysi-ikäisyydestä ja sukupuolesta paljastamatta henkilön henkilötunnusta tai edes tarkkaa ikää.

Itsehallittavassa mallissa luottamus henkilötietoihin on toteutettu **hajautetun tilikirjan** (engl. decentralised ledger technology, DLT) avulla. Hajautetut tilikirjat on laajeneva teknologiaperhe, josta laajimmin tunnetut lohkoketjut, kuten Ethereum tai Blockchain, ovat osajoukko. Yksilöiviä henkilötietoja ei koskaan tallenneta julkiseen tilikirjaan, mutta palvelu attribuuttitietojen pyytäjänä varmentaa tilikirjasta julkisen tahon (oikeushenkilön) myöntämän kryptografisen julkituonnin paikkansapitävyyden ja voimassaolon. Varmentaminen perustuu **hajautetun julkisen avaimen** (engl. Decentralised Public Key Infrastructure, DPKI) menetelmiin.[3]

Hajautettu tunniste (engl. Decentralised Identifier, DID[4]) on yksilöllinen, pseudonymisoitu tunniste, jonka avulla identiteetin omistaja voi tunnistautua organisaation tarjoamissa palveluissa, ja joka voidaan liittää väitteisiin sekä julkituonteihin, mutta jota rekisterinpitäjä tai ulkopuolinen ei voi yksipuolisesti yhdistää luonnolliseen henkilöön.

Väite on identiteetin omistajan jakama, tätä koskeva standardimuodossa kerrottu tieto (katso myös **attribuutti**). Jos oikeellisuus on todennettavissa väitteen myöntäjän kryptografisesta allekirjoituksesta kyseessä on **varmennettava väite** (engl. credential, verifiable credential).

Julkituonti on (varmennettavia) väitteitä yhdistelemällä tai laajempaa väitettä rajaamalla muodostettu tieto (engl. proof), josta löytyy ainoastaan tapahtuman kannalta tarpeelliset tiedot (engl. selective disclosure). Tieto ei aina muodosta henkilötietoa - esim. abstrakti tieto *asuu Helsingissä* ei julkituontina ilman muita attribuutteja paljasta identiteetin omistajan henkilöllisyyttä, jollei konteksti ole ilmeinen (esimerkiksi vain kaksi hakijaa opiskelupaikkaan, joista toinen ulkomailta).

Minimaalinen identiteetti (tai **attribuutiton identiteetti**) on yksilöivä tunniste jolla yksilö voidaan tuoda (rajatusti) palvelujen piiriin ennen roolin ja siihen liittyvien tarkentavien attribuuttien syntymistä.

---

[3] Jyrki Pitkänen. Itsehallittavan identiteetin sääntely EU:n yleisessä tietosuoja-asetuksessa. Lapin yliopiston notaaritutkielma 2018.

[4] Decentralized Identifiers (DIDs), World Wide Web Consortium, https://w3c-ccg.github.io/did-spec/

2.5 Käyttäjäkeskeisen identiteetinhallinnan ydinvaatimukset

Euroopan komission rahoittamassa eduKEEP-projektissa on tutkittu käyttäjäkeskeisen identiteetinhallinnan hyödyntämistä korkeamman opetuksen ja tutkimuksen yhteydessä - tässä kontekstissa ratkaisuille on muodostunut yleinen termi **eduID**. Projektissa on luonnosteltu alla luetellut perustavan tason vaatimukset käyttäjäkeskeiselle identiteetinhallinnalle:

Itsehallinnoitavuus (User-Managed)
Identiteetti (tai tunniste) on henkilön itse luotavissa, ja perustietojen (nimi ja toimiva sähköpostiosoite) osalta itse ylläpidettävissä. Tämän pohjaidentiteetin avulla henkilö voi luoda yhteyksiä ja käyttäjäoikeuksia yhtäaikaisesti useisiin oppimisen instituutioihin, joiden kanssa hän on tekemisissä, olettamuksella, että henkilö pystyy suoraan vastaamaan näiden instituutioiden palvelujen asettamiin todentamiskriteereihin, tai nostamaan tunnistautumisensa luotettavuustasoa eduID-järjestelmän itse tarjoamissa puitteissa.

Pysyvyys (Persistent)
Elinikäisen oppimisen tukemiseksi identiteetti liittyy omistajaansa pysyvästi. Järjestelmä ei saa vaatia uuden identiteetin luomista oppilaitoksesta toiseen siirryttäessä tai toimittaessa useammassa yhtäaikaisessa organisaatiossa. Pysyvyys tulee taata riippumatta henkilön elämäntilanteiden muutoksista.

Tietosuojalähtöisyys (Privacy Preserving)
Oppija hallinnoi itse hänestä olemassa olevien attribuuttien käyttöä eri organisaatioiden yhteydessä. Attribuuttien toimittaminen tapahtuu turvallisesti (suojattua kanavaa käyttäen) ja käyttäen vain pienintä tarvittavaa määrää attribuutteja. Attribuuttitiedon minimoinnin hallinta ja julkaiseminen on keskitetyissä nykyratkaisuissa aina organisaation, ei oppijan vastuulla ja tarkoittaa myös oppijan suostumuksen hankintaa attribuuttien käytölle kolmansien osapuolten kanssa toimittaessa.

Organisaatioiden tukema (Institutionally Backed)
Käyttäjäkeskeinen oppimisen tunniste tarvitsee itsehallittavuuden rinnalle tuen koulutus- ja tutkimusorganisaatioilta. Niiden tulee pystyä toimittamaan luotettavasti tietoja oppijoistaan ja tutkijoistaan identiteetinhallintajärjestelmänsä kautta. Toisin kuin nykyjärjestelmä, joka yhdistää identiteetin ja opiskelu- tai työsuhteen (affiliaation), käyttäjäkeskeisessä identiteetinhallinnassa organisaatioista tulee käyttäjätietojen välittäjiä- Oleellinen elementti tässä vaatimuksessa on organisaation oma luotettu identiteetti, kuten X.509-pohjainen varmenne tai oma julkinen hajautettu tunniste.

3 Ratkaisuehdotus

3.1 Kohti käyttäjäkeskeistä identiteetinhallintaa

Selvityksen perusteella ehdotamme, että Suomen koulutustoimialalla alettaisin varautua jatkuvan oppimisen asettamiin haasteisiin keräämällä lisätietoa
käyttäjäkeskeisen identiteetinhallinnan mallista. Ensiaskel on järkevä ottaa keskitetyn käyttäjäkeskeisen identiteetinhallinnan mallista, josta on tehty toteutuksia Ruotsin ja Sveitsin korkeakoulufederaatioissa (ks. luku 4.1).

Keskitetyn käyttäjäkeskeisen identiteetinhallinnan mallin etuja ovat:

- Joustavampi liikkuvuus eri organisaatioiden välillä, kun sähköinen identiteetti ei ole sidottu yhteen organisaatioon kerrallaan
- Käyttäjäystävällisyys, kun samalla tunnistuspalvelulla voi tunnistautua mahdollisimman moneen palveluun
- Mahdollisuus rakentaa helppokäyttöinen siirtymispolku nykyisistä luottamusverkostoista (Haka ja MPASSid) käyttäjäkeskeiseen ratkaisuun sadoilletuhansille käyttäjille
- Harmoniassa EU:n tietosuoja-asetuksen kanssa, joka korostaa rekisteröidyn oikeutta omien tietojen hallintaan
- Mahdollisuus siirtyä helposti itsehallittavan identiteetin ratkaisumalleihin (sekä nopeissa eurooppalaisissa kokeiluissa ja laajemmassa käytössä pidemmällä aikavälillä)

Ratkaisuehdotus on laadittu arvioimalla luvussa 4 käsiteltyjä hankkeita Suomessa ja maailmalla. Oleellisia teknis-taloudellisia arviointiparametrejä ehdotuksen suuntauksessa ovat olleet:

- Kansainvälinen yhteentoimivuus jo olemassa olevien akateemisten tunnistusratkaisujen kanssa (kansalliset federaatiot, ORCID id, eduID:t)
- Kansainvälinen yhteentoimivuus kansallisten ja EU-tason (eIDAS) kansalaisen vahvojen tunnistusratkaisujen kanssa
- Oppijatunnisteen pysyvyys (arvio tunnisteen tarpeesta 50-80 vuoden ajaksi)
- Tunnisteiden korreloimattomuus ja yksikäsitteisyys
- Ratkaisuarkkitehtuurin vikasietoisuus
- Teknologian kypsyystaso
- Teknologian käyttöönoton ja ylläpidon kustannukset
- Teknologian kehitystyökalut ja ekosysteemivahvuudet

Käyttäjäkeskeiseen identiteetinhallintaan siirtyminen on iso muutos, joka aiheuttaa paljon uusien toimintatapojen opettelua niin käyttäjille, koulutusorganisaatioille kuin palveluntarjoajille. Siirtymää voidaan helpottaa hyödyntämällä välivaiheena keskitettyä, mutta käyttäjäkeskeistä identiteetinhallintaratkaisua, johon voidaan rakentaa käyttäjän näkökulmasta helppo, ohjattu siirtyminen nykyisistä koulutustoimialan luottamusverkostoista, kuten Hakasta ja MPASSid:sta.

Esitetty ratkaisu tarkoittaa hallitun askeleen ottamista kohti käyttäjäkeskeistä identiteetinhallintaa. Keskitetyn tahon ylläpitämä palvelu, jossa vahvasti ensitunnistettuun sähköiseen identiteettiin voidaan linkittää hajautetusti eri lähteistä myönnettäviä attribuutteja sisältää lyhyellä tähtäimellä vähemmän riskejä käyttövarmuuden ja -turvallisuuden kannalta kuin siirtymä kertaheitolla nykymaailmasta itsehallittuun identiteetinhallintaan (SSI). Syitä keskitetyn ratkaisun suosimiseen itsehallittavan identiteetin asemesta on

1. lainsäädännön vielä ratkaisemattomissa haasteissa,
2. identiteettilompakoiden käyttäjäkokemuksen toteuttamiseen liittyvissä puutteissa,
3. hajautettujen lompakkoratkaisujen varmuuskopiointiin liittyvissä avoimissa kysymyksissä ja
4. tunnistamisparadigman vahvassa olettamassa yksilön kykyyn kantaa täysi vastuu omien identiteettiattribuuttien hallinnoinnista.

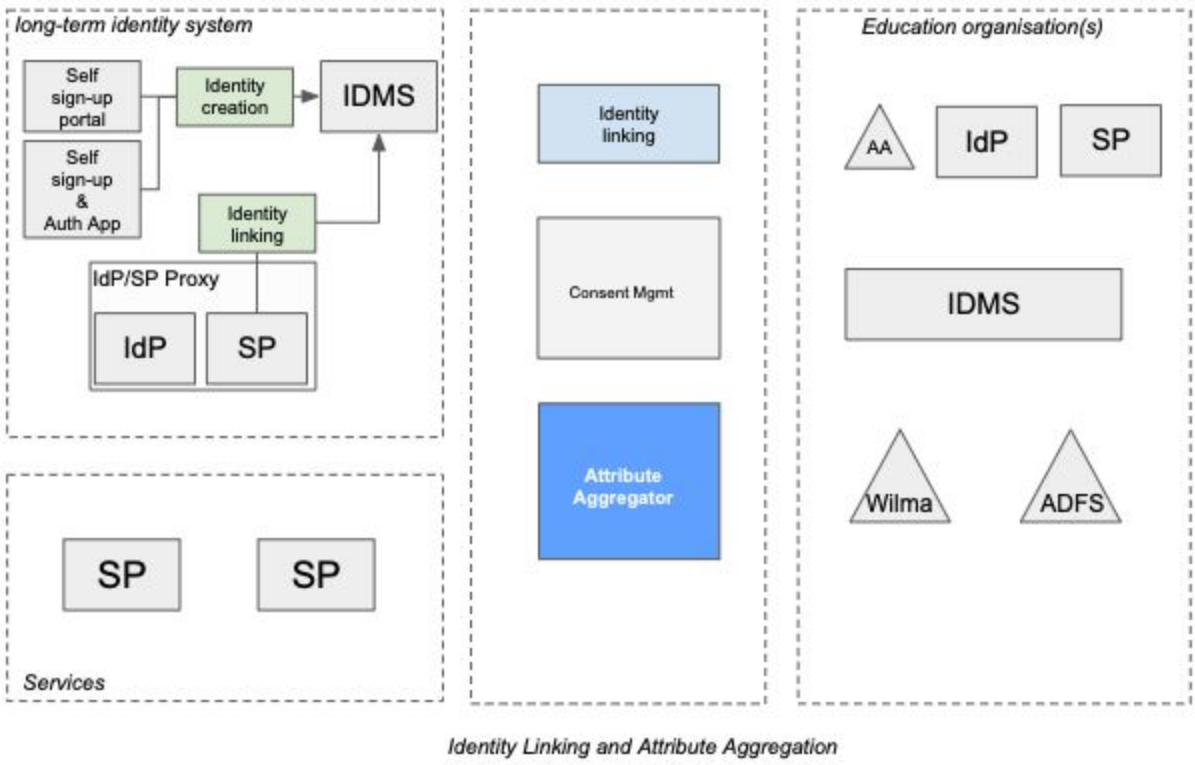
Selvityksessä esitelty Sandbox of Trust -hankkeen SisuID-tunnistusratkaisu (ks. luku 4.1.1) on keskitetty käyttäjäkeskeinen identiteetinhallintaratkaisu, jonka ympärille on syntymässä laaja yksityisistä ja julkisista toimijoista koostuva yhteistyöverkosto. Ehdotamme, että koulutustoimiala pyrkisi yhteistyöhön SisuID:n yhteistyöverkoston kanssa sen asemesta, että alkaisi kehittää omaa ratkaisua. Erityisesti älypuhelinsovelluksen kehittäminen edellyttää erityisosaamista, jota koulutustoimialan toimijoilla ei perinteisesti ole ollut. .

Esitetty ratkaisu täydentäisi SisuID:ta lisäämällä siihen toiminnallisuuden, jonka avulla SisuID:n pitkäaikaiseksi tarkoitettuun perusidentiteettiin voisi kytkeä eri organisaatioiden tuottamia käyttäjätietoja (attribuutteja tai väitteitä).

3.2 Ehdotuksen rajaukset

Ratkaisuehdotuksessa on tehty alla luetellut rajaukset:

- Toteutetaan koulutustoimialalla tarvittavien käyttäjätietojen välityspalvelu. Sen perusidea on yhdistää käyttäjän luoma pysyvä sähköinen identiteetti koulutustoimialan palveluiden kannalta oleellisiin käyttäjätietoihin, kuten kansalliseen oppijanumeroon ja rooliin tietyssä oppilaitoksessa (“käyttäjä on 7A-luokan oppilas Mäntymäen koulussa”, “käyttäjä on luonnontieteiden jatko-opiskelija Helsingin yliopistossa”)
- Käyttäjätietojen välityspalvelu suunnitellaan niin, että se voidaan ottaa kansalliseen käyttöön koulutustoimialan lisäksi myös muilla toimialoilla.
- Käyttäjätietojen välityspalvelulla pyritään ratkaisemaan ensi sijassa organisaatioiden välisiä käyttäjäntunnistuksen käyttötapauksia.
- Toteutuksessa huomioidaan koulutustoimialan luottamusverkostot Haka ja MPASSid, sekä niissä tehdyt määrityksen ja sopimukset. (MPASSid-ratkaisusta tarkemmin tämän selvityksen kappaleessa 4.3.1).
- MPASSid-tunnistusratkaisussa tehdyt laajennukset Shibboleth IdP -ohjelmistoon voisivat toimia tässä arkkitehtuurissa esitetyn teknisen ratkaisun toteuttamisen perustana.



Kuva 3. Sähköisten identiteettien linkitys ja käyttäjätietojen välitys oppilaitosten omistamien identiteettien ja käyttäjän itse luoman pitkäikäisen sähköisen identiteetin välissä.

Ehdotuksen tekninen tutkintalinja selvittäisi pienellä käyttäjäjoukolla sähköisten identiteettien linkitystä ja käyttäjätietojen välittämistä teknisenä pilottina. Testihenkilöille luotaisiin SisuID-identiteetit, jotka kytkettäisiin pilotoitavalla identiteettien linkityksen ja käyttäjätietojen välityksen palvelulla (identity linking ja attribute aggregator kuvassa 3 yllä) testihenkilöiden sähköisiin identiteetteihin testioppilaitoksissa. Linkityksen onnistuminen voitaisiin demonstroida kirjautumalla pilottipalveluun SisuID-tunnistuspalvelulla, joka saisi käyttäjätietoa pilotoivalta identiteettien linkityksen palvelulta. Teknisen tutkintalinjan mahdollistava tekninen arkkitehtuuri on hahmoteltu tarkemmin luvussa 3.3 alla.

Ehdotuksen hallinnollis-juridinen toimintalinja selvittäisi millaisia lakeihin, sopimuksiin ja teknisiin määrityksiin liittyviä asioita pitäisi ratkaista, jotta käyttäjäkeskeiseen identiteetinhallintaan voitaisiin siirtyä. Selvitettäviä asioita olisivat mm.

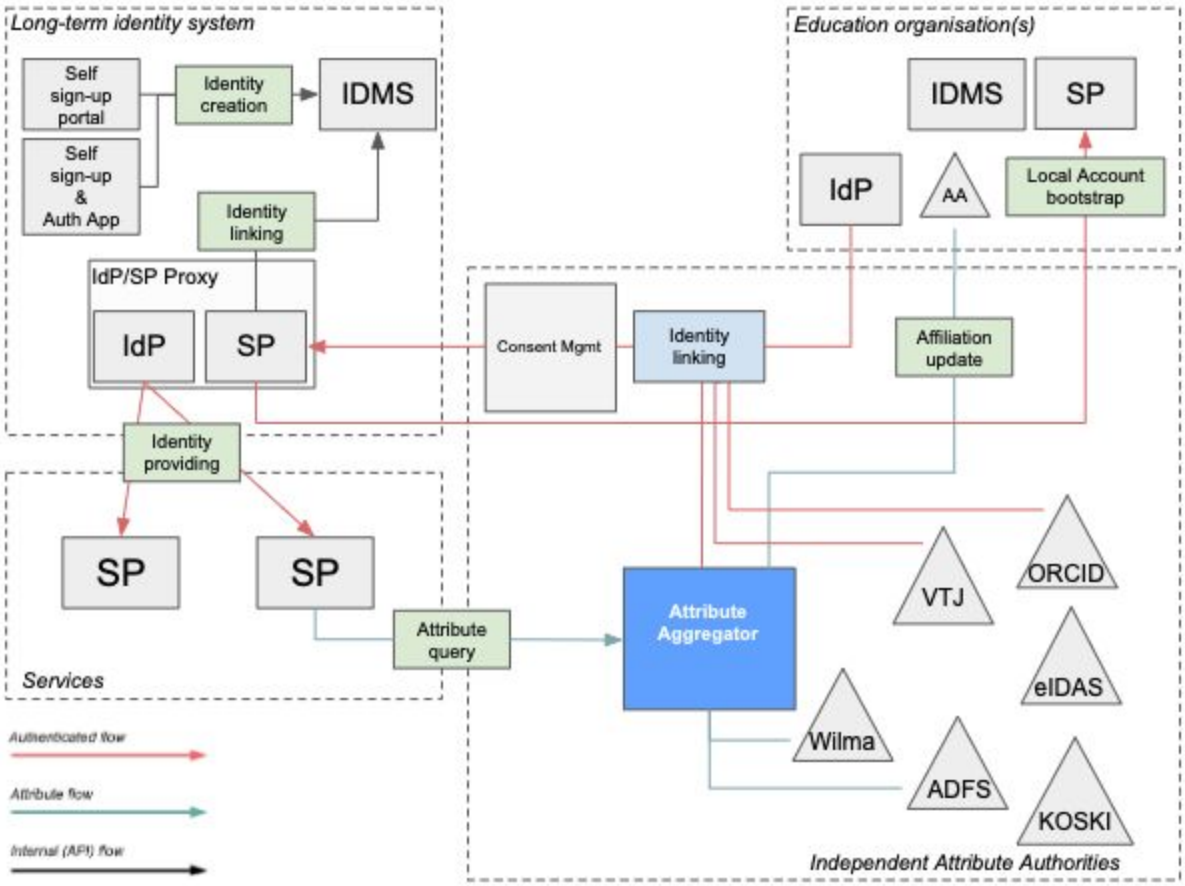
- Henkilötietojen juridiikka toisiokäytettäessä oppilaitosten tai Opetushallituksen Koski-palvelun tietoja jatkuvan oppimisen digitaalisissa palveluissa käyttäjäkeskeisen identiteetinhallintamallin kautta. Selvitys täydentäisi valtiovarainministeriön Yhteisen tiedon hallinta -hankkeessa tehtyä selvitystä Omadata julkishallinnossa. Lisäksi

selvitettäisiin Haka-luottamusverkoston jäsensopimuksen ja MPASSid-luottamusverkoston jäsensopimuksen mahdollisesti asettamat juridiset rajat käyttäjäkeskeiseen identiteetinhallintaan siirtymiselle.

- Välitettävien tietojen muodon ja merkityksen määritykset. Tässä olisi mahdollista saada tuloksia nopeasti vertaamalla Haka-luottamusverkoston käyttäjätietojen määritystä ja MPASSid-luottamusverkoston käyttäjätietojen määritystä ja keinoja yhteismitallistaa niitä. Jatkuvan oppimisen palveluita tuottavia tahoja tarvitaa validoimaan määritykset.
- Käytännön toimintamallien määritykset esimerkiksi tunnistusvälineen käyttöönottoon. Suomessa olisi mahdollista sopia tehokas kansallinen ensitunnistuksen ja tunnistusvälineen käyttöönoton toimintamalli esimerkiksi esiopetukseen ilmoittautumisen yhteydessä.

3.3 Arkkitehtuuri

Arkkitehtuuriehdotuksen päämääränä on toteuttaa luvussa 2.5 esitetyt käyttäjäkeskeisen identiteetinhallinnan ydinvaatimukset siten, että se olisi toteutettavissa mahdollisimman vähällä lisätyöllä. Tämä tavoite saavutetaan hyödyntämällä jo valmiita koulutustoimialan ratkaisuja kuten Haka, MPASSid ja KOSKI-palvelu, ja suomalaisten yritysten ja julkishallinnon yhteistoimin kehittämiä keskitetyn identiteetinhallintamallin mukaisia konsepteja jotka hyödyntävät OpenID Connect -teknologiaa (merkitty kuvassa 4 alla “Long-term identity system”). Tällaisia käynnissä olevia hankkeita ja kokeiluja ovat Teknologiateollisuuden vetämä Sandbox of Trust ja Suomen Tilaajavastuu Oy:n MyData-lompakko.



Kuva 4. Käyttäjäkeskeisen oppijaidentiteetin hallinnan arkkitehtuuri (roolit SAML-terminologialla).

Selvennys ehdotetun arkkitehtuurin kokonaisuuksista ja rooleista:

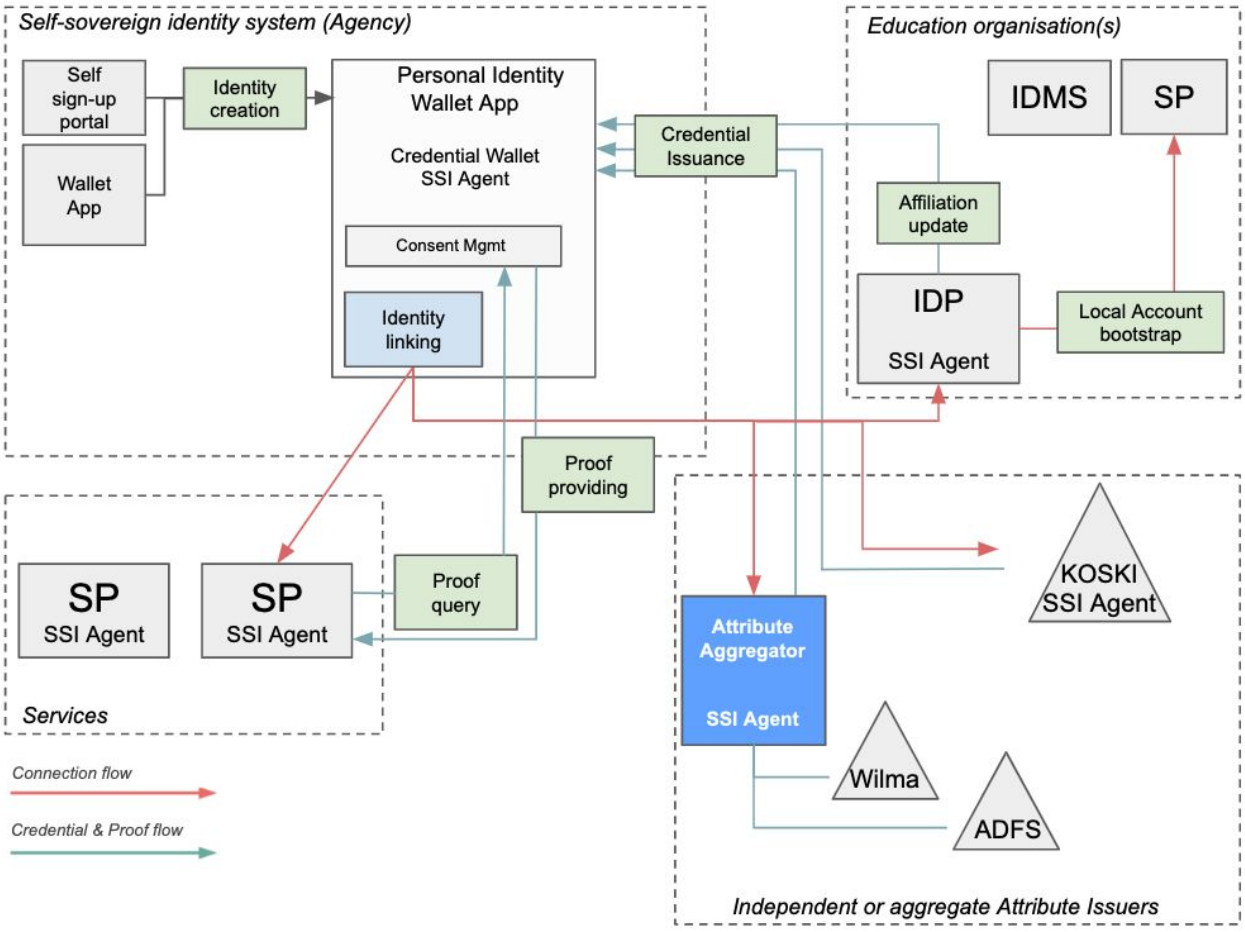
Identiteetin luominen ja tarjolla olevat turvalliset tunnistusmenetelmät (sovelluksen käyttämät biometriset tunnisteet jne.) kuuluvat kuvassa 4 **Long-term identity system-osioon**. Käyttäjälle on tarjolla (yksi tai useampi) tunnistuspalvelu, jossa käyttäjä voi luoda itselleen sähköisen identiteetin ja tunnistautua esim. älypuhelinsovelluksella. Keskitetty yksikäsitteiset tunnisteet sisältävä tietokanta ylläpidetään tämän osion alle kuuluvassa tunnistetietokannassa (IDMS). Edellämainittu osio tarjoaa tunnistamispalvelun (IdP/SP Proxy) tunnistamista hyödyntäville palveluille (**Services-osio**), jotka voivat tunnistuksen avulla saatavan tokenin avulla tehdä attribuuttikyselyjä oppijan linkittämiin ja luvittamiin tietolähteisiin.

Tunnistamispalvelu tarjoaa mahdollisuuden linkittää useita paikallisia identiteettejä ja attribuutteja tarjoavia palveluja yhden keskitetyn tunnisteen alle. Käytettävä perustunniste voisi olla esimerkiksi Kansallinen oppijanumero tai VM:n asettaman Henkilötunnuksen uusiminen -työryhmän väliraportissa mainittu uusi yksikäsitteinen henkilötunnus. Oleellista on, että jatkuvan oppimisen maailmassa tunnisteen pitää olla pitkäikäinen mieluiten oppijan koko eliniän kestoinen. Linkitettäviä identiteettejä ovat esim. nykyiset MPASSid:n välittämät tunnisteet ja

paikalliset käyttäjätunnukset koulutusjärjestelmissä (**Education organisation -osio**). Paikallisten käyttäjätunnusten luonti näissä organisaatioissa voitaisiin käynnistää tunnistamispalvelun tarjoaman perusidentiteetin pohjalta, kuten Ruotsalaisten eduID-järjestelmässä tehdään nyt yliopistojen käyttäjätunnusten osalta.

Järjestelmän oleellinen identiteetinhallinnan mekanismi on perustunnisteeseen ajan kuluessa liitettävät (luotavat, uusittavat, poistettavat tai ekspiroituvat) attribuutit, joiden myöntäjiä ovat luotetut organisaatiot (julkiset attribuuttiauktoriteetit, **Independent attribute authorities -osio**). Attribuutteja aggregoivan välityspalvelun kautta tarjolla olisi paikallisten koulutustoimijoiden käyttäjähallinta- ja tunnistuspalvelujen identiteettejä ja attribuutteja. Oppimisen järjestelmissä tarvittavia attribuutteja tarjoaisivat sopivaa tunnistustasoa vastaan myös VTJ, KOSKI, Traficom, YTJ (käytössä vahva tunnistaminen), ORCID ja mahdollisesti federoitavat maakohtaiset eduID-palvelut (joissa on käytössä yksi- tai kaksivaiheinen tunnistaminen (engl. Single-Factor Authentication (SFA) ja Two-Factor Authentication 2FA)).

Kuvassa 4 kuvatun arkkitehtuurin toteuttamisen avulla ennakoidaan ja mahdollistetaan attribuuttipohjaiseen tunnistamiseen siirtymisellä jouheva siirtymä hajautetun itsehallittavan identiteetin käyttöön 3–10 vuoden sisällä, myös jatkuvan oppimisen ja siihen liittyvien atribuuttien osalta. Viimeksi mainitun siirtymän hajautettuun arkkitehtuuriin (kuva 5) voi mahdollistaa valtio tai joku muu toimija joka tarjoaa keskitetyn mallin sijaan täysin hajautetun mallin mukaan toteutetun tunnistusvälineen (identiteettilompakon) ja tunnisteet (DID:it) joita käytettäisiin sekä luonnollisten henkilöiden että oikeushenkilöiden yhteydessä. Yksinkertaisin siirtymä voi tarkoittaa SisuID-mobiilisovelluksen muuntamista identiteettilompakoksi, jossa hajautetun identiteetin omistaja hallinnoi tunnistamisessa tarvittavia attribuutteja jotka on muunnettu sopivan organisaation tai organisaatioiden myöntämiksi varmennettaviksi väitteiksi. Väitteiden ja tunnistamisvälineen käytössä ei tällöin tarvita keskitettyä tietokantaa ylläpitävää operaattoria pitkäaikaisen identiteetin ylläpitäjäksi. Eri tyyppisiä väitteiden myöntäjiä ja näille määriteltyjä luottamusverkostoja sen sijaan tarvitaan, ja tässä voidaan hyödyntää jo aiempia attribuuttitoimittajien verkostoja ja keskinäisiä luottamusverkkosopimuksia.



Kuva 5. Käyttäjäkeskeinen identiteetinhallinta itsehallittavan identiteetin arkkitehtuurilla toteutettuna. Palvelujen identiteetti ja myöntämät väitteet voidaan tarkistaa hajautetusta tilikirjasta kuten FIndy (joka ei kuvassa).

3.4 Vaiheistus

3.4.1 Nopea pilotointi SisuID:n kanssa

Selvityksessä tehtyjen johtopäätösten perusteella ensimmäinen konkreettisesti otettava askel on Sandbox of Trust -hankkeen, OKM:n ja tämän selvityksen tekijöiden välillä järjestettävä keskustelu ehdotetun arkkitehtuurin validoinnista nopeasti ja ketterästi; oleelliselta osin MPASSid-tunnisteiden ja nykymuotoisen tunnistamispalveluproxyn muuttaminen attribuuttien välittäjäksi ulkopuoliselle eID-palvelulle (Sandbox of Trustin oma identiteettioperaattori). Jos tämä osoittautuu mahdolliseksi esimerkiksi Sandbox of Trust -hankkeen käyttötapauspilottina, tulee harkita hankkeeseen liittymistä ja jatkotyön tekemistä sen yhteydessä. Hankkeeseen liittyy myös riskejä kuten mahdollinen epäonnistuminen ensitunnistamisprosessin sertifioinnissa tai sovittavan hallintomallin ja tunnistamiskustannusten (vuositasolla maksettava, käyttövolyymipohjainen jäsenmaksu) liikkumaväli. SisuID on arkkitehtuurissa tarvittaessa

helposti korvattavissa toisella vastaavan toiminnallisuuden tarjoavalla eID-ratkaisulla, jos niitä tulee tunnistusmarkkinaan tarjolle.

3.4.2 Itsehallittavan identiteetin kokeilut

Itsehallittavia identiteettejä varten luodaan Suomeen FIndy-nimistä hajautetun tilikirjan (ledgerin) käyttöön perustuvaa identiteetti-infrastruktuuria, ensimmäisissä käyttötapauksissa ledgerin avulla julkisia hajautettuja tunnisteita luodaan vain oikeushenkilöille. Nopean SisuID:n kanssa tehtävän pilotoinnin jälkeen toteutettavan itsehallittavaa identiteettiä soveltavan pilotin mahdollistamiseksi olisi FIndy-infraan luotava esimerkiksi KOSKI-palvelulle oma hajautettu organisaatiotunniste ja sen kautta löytyvä ns. yrityslompakko (engl. enterprise wallet). Myös kohdan 3.4.1 pilotissa kokeiltava välityspalvelu voitaisiin nähdä tässä kokeilussa organisaationa joka myöntää edelleen attribuutteja, mutta nyt toisessa muodossa. Varmennettavia väitteitä myöntävälle auktoriteetille kuten KOSKI-palvelu tai edellisen vaiheen toteuttama välityspalvelu tulisi määritellä asema FIndyn toimintaa hyödyntävässä luottamusverkossa, toisin sanoen myöntäjästä tulisi ‘leimata’ luottamusankkuri (engl. Trust Anchor) sen myöntämien väitteiden osalta. Toteutus tapahtuu tältäkin osin varmennettavilla väitteillä, jotka ovat rinnastettavissa sähköisiksi sopimuksiksi tilikirjasta löytyvien, julkisten organisaatioiden välillä; OKM myöntämä väite välityspalvelulle sallii sen myöntää tiettyjä koulutusasteen attribuutteja. Myöntöoikeus voidaan tarvittaessa poistaa reaaliaikaisesti, revokoimalla ao. väite tilikirjan avulla.

Kokeilun osana tulee määritellä ainakin osa nykyisistä oppijoihin liittyvistä koulutusalan attribuuteista myös tarvittavien uusien tietomallien mukaisiksi - toteuttaa siis tietomalli- ja attribuuttikonversio Haka & MPASSid palvelujen SAML-attribuuteista joko Indy (tai W3C Verifiable Credential) -määritysten mukaisiksi varmennettavien väitteiden skeemoiksi ja väitemäärittelyiksi.

Jos koetaan tarpeelliseksi muodostaa nopeasti näkemystä ja teknistä osaamista itsehallittavien identiteettien ja hajautettujen tunnisteiden käytöstä mobiililompakon avulla, on hollannissa kokeiltavaan IRMA-ratkaisuun (ks. alaluku hankeselvitysluvussa 4) pohjautuva pilotti yksi toteutettavissa oleva vaihtoehto. Helsingin yliopisto on jo mukana IRMAn määrittämien tunnistamisen mahdollistavien attribuuttien myöntämisessä hollantilaisten koulutusorganisaatioiden lisänä, samoin eduGAIN, johon CSC:llä on läheiset yhteydet. Suomessa tehtäviin pilotteihin IRMA eID-mobiilisovellus tulisi tosin saada jakeluun myös Suomen App Storeen ja Google Play:hin.

Alla alustavina ehdotettuihin pilottiaihioihin tulisi kehittää lähestymistavan teknisen toteutuksen ja haetun käyttäjäkeskeisyyden todentamisen- kannalta hyödyllinen käyttötapaus ja siinä oleellisesti tarvittavat käyttäjäattribuutit. Luonnollisesti tulee huomioida voimassaolevat tietosuojasäädökset ja tiedon minimointiperiaate.

Jos testataan useampaa teknologiaratkaisua, kannattaa kunkin validoida eri käyttötapaus.

Pilotti-idea	**SisuID ja Haka/MPASS attribuuttien aggregointi**	**IRMA-mobiilisovellus eID-tunnisteena**	**KOSKI-palvelun myöntämät varmennettavat väitteet**
Toimijat + kumppanit	Sandbox of Trust-hanke + CSC + OPH	eduGAIN, HY + CSC	FIndy + OPH + Sandbox of Trust-hanke
Ehdotettu pilotti/käyttötapaus keskustelun pohjaksi	*DigiSuomi:Opintojen aloittaminen* (tunnisteen käyttöönotto ja käyttö alaikäisenä ja/tai Ulkomaalaisen ELIXIR-AAI opiskelijan vahva ensitunnistaminen)	Identiteettilompakon UX-analyysit, ekosysteemin kehittäjäkokemus-analyysi	Indy-lompakkoon myönnettävät oppijan attribuutit (sama käyttötapaus kuin SisuID:ssä) ja/tai Compleap ja tutkintopätevyys varmennettavana väitteenä
Teknologia	OpenID Connect, SAML, SisuID identity enrolment/proofing	IRMA-muotoiset varmennettavat attribuutit	Hyperledger Indy, Indy-muotoiset varmennettavat attribuutit ja agentit, Indy-tunnistelom-pakko (SisuID?)
Synergia- ja verkostoedut	Yhteisö muodostumassa (Nixu, CSC, OKM, VRK)	HY-IRMA kokeilu, ei muita	Osin sama yhteisö kuin SisuID:ssä, Indy on osa SisuID:n evoluutiopolkua
Ehdotettu priorisointi (1-2-3)	1	3	2

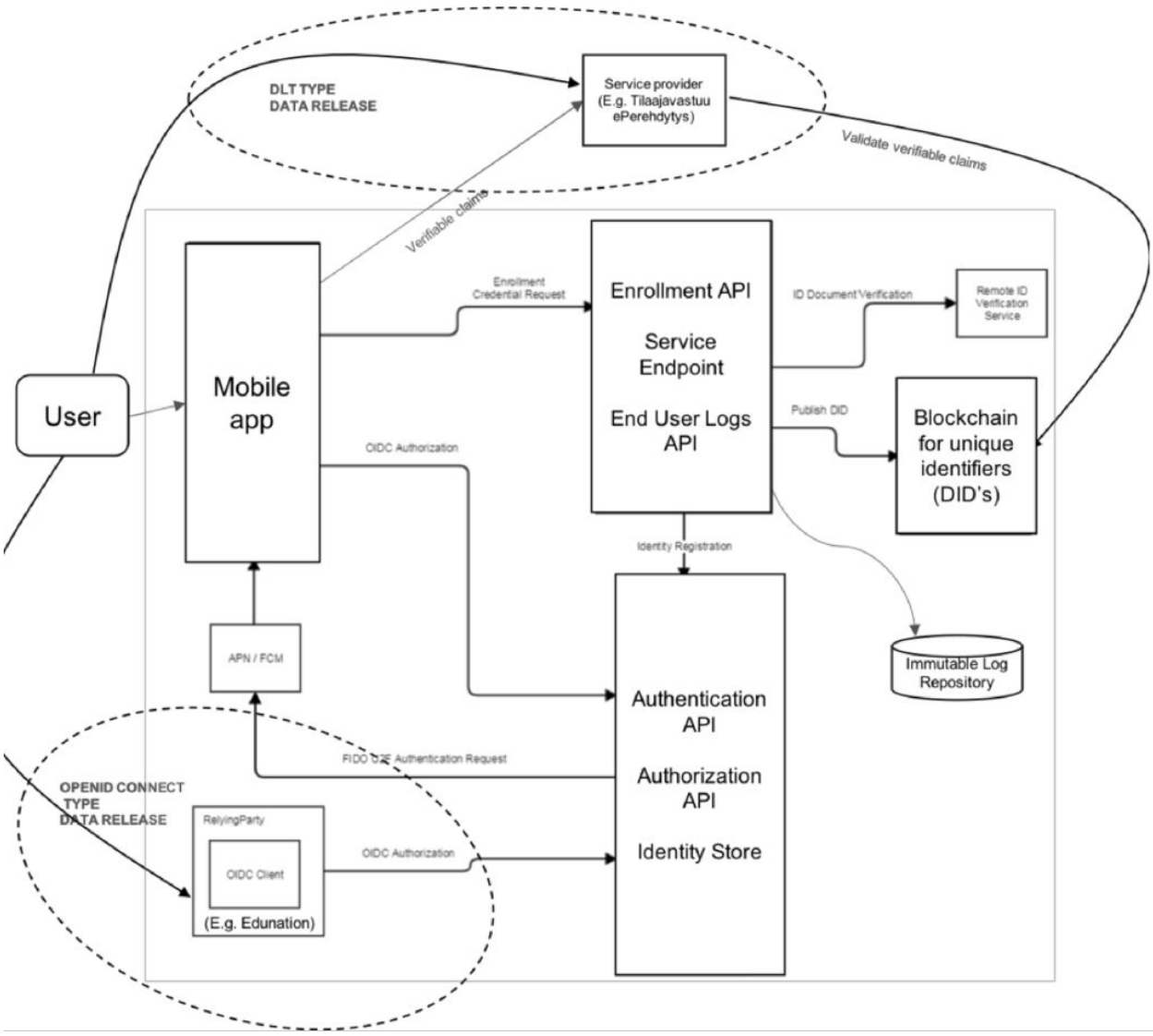
4 Selvityksessä analysoidut hankkeet

4.1 Keskitetyt käyttäjäkeskeiset tunnistusratkaisut

4.1.1 SisuID (Sandbox of Trust)

Teknologiateollisuuden vetämän RTECO-hankkeen osallistujien piiristä syntyi 2018 kesän aikana uusi hanke Sanbox of Trust (“SoT”) jossa on tarkoitus luoda Suomelle uusi alemman ja vahvan tunnistautumisen mobiilisti toteuttava ratkaisu ja hallinnointimalli. Vetureina hankkeessa on Teknologiateollisuuden lisäksi identiteetinhallinnan yrityksiä Pohjoismaista - Digital Living Oy, Nixu Oy, Suomen Tilaajavastuu Oy ja Tieto Oyj.

Idea on lähtenyt liikkeelle tarpeesta vastata erityisesti talouskasvulle tärkeän kansainvälisen työntekijä- ja opiskelijaliikkuvuuden tarpeisiin. Tavoite on ratkaista kustannustehokkaammin hankala ja kallis vahvan tunnistamisen (eIDAS-varmistustaso LoA2, “substantial”) ensitunnistaminen ulkomaalaisille jotka tarvitsevat vahvaa tunnistautumista asioidakseen tai hankkiakseen toimeentulonsa Suomessa - alue johon nykyisin ensitunnistamisen toteuttavilla pankeilla ei ole liiketoiminnallista insentiiviä. Tulos on onnistuessaan helppokäyttöinen ja samalla riittävän luotettava ensitunnistamisen prosessi kansainvälistä liikkuvuutta hyödyntäville opiskelijoille ja esimerkiksi työelämän liikkuville ammattilaisille.



Kuva 5. Sandbox of Trust -systeemiarkkitehtuurimalli (Copyright Sandbox of Trust -konsortio).

Käyttäjälle on ideoitu SoT-identiteettinsä hallintaan mobiilisovellus, jolla käyttäjä voi tunnistautua SoT-yhteensopivissa palveluissa. Identiteetin luonti- ja hallintapalvelut toimivat keskitetysti, ja niitä operoisi tietosuojavaatimukset täyttävä sertifioitu ja auditoitu organisaatio. Teknisesti järjestelmässä on sekä perinteisen tunnistautumispalvelun ja itsehallittavan identiteetin ominaisuuksia, jälkimmäisen rooli ei näytä mallissa vielä kovin selkeältä.

Tarjolla Sandbox of Trustin käyttäjäkokeiluksi on ollut pilotti-idea jossa ulkomailta Suomeen saapuvan opiskelijan identiteetti todennettaisiin opiskelijapaikan vastaanottamisen yhteydessä ilman fyysistä vierailua Suomessa. Oleellinen huomio konseptissa on vaadittavien henkilöllisyysdokumenttien toimittaminen sähköisesti opiskelemaan tulevan henkilön asentaman mobiilisovelluksen (kameran ja skannaustyökalujen) ja rajapinnan kautta (“enrolment API”)

edelleen Keesing Technologies:in teknologiaan pohjautuvalle, ensitunnistamisesta vastaavalle keskitetylle palvelulle (kuvassa 5 “Remote ID Verification Service”). SoT:n pilotissa kehitettävä identiteetin etätodentamispalvelu auditoidaan Ficoran ja eIDAS:n vahvan tunnistamisen vaatimuksia vasten - lopputuloksena tavoite verifioida minkä varmistustason (AL1 vai AL2) konseptoitu etätunnistusratkaisu mahdollistaa. Verifioitu identiteetti kirjataan attribuutteineen OpenID Connect -pohjaisen keskitetyn IAM-järjestelmän tunnistetietokantaan.

Käyttäjä voi vahvistaa sisäänkirjautumisen SoT-tunnistamista hyödyntävään palveluun mobiilisovelluksella, mahdollisia tunnistautumistasoja olisi kaksi - AL1 ja AL2. Lisäksi sovelluksella on (arkkitehtuurikuvan perusteella) tarkoitus pystyä toimittamaan niitä pyytäville palveluille varmennettavia väitteitä. Tämä tarkoittaisi esimerkiksi Hyperledger Indyn tarvitseman agentti- ja lompakkoteknologian integrointia mobiilisovellukseen.

Yksittäisille käyttäjille aina ilmaisen SoT-sovelluksen käytön ja Enrolment-palvelun aiheuttamat kustannukset on tarkoitus kattaa tunnistusalustan hyödyntäjien maksamalla kiinteällä, tunnistusvolyymiin porrastetulla jäsenvuosimaksulla. Kustannusarvio vaadittavat auditoinnit ja sertifioinnit täyttävän toimijan osalta on vuositasolla alle 10 MEUR.

Tuotantoon päädyttyään SoT-palvelut on tarkoitus järjestää voittoa tuottamattomana osuuskuntana, ja hinnoittelu- ja vastuurahastot sovitaan sen sääntökirjassa. Jäsenistö sopii hinnoittelun vuosittain, ja jakaa toiminnasta syntyneet kustannukset ja riskit.

SoT-konsortion kaavailema liiketoimintamalli on merkittävä disruptio verrattuna kansallisen vahvan tunnistamisen luottamusverkoston nykyiseen säännöstöön - esimerkkinä esimerkiksi vahvan ensitunnistamisen nykyinen laissa säädelty hinnoittelumalli jossa tunnistamisesta syntyneet kulut (usein ei täysimääräisesti) korvataan pankeille tapahtumavolyymipohjaisesti (nykyhinta 2,51 EUR/ensitunnistus. Hintaa on ehdotettu alennettavaksi uudessa VM:n laatimassa hallituksen esityksessä 13 senttiin).

Johtopäätös jatkuvan oppimisen identiteetinhallinnan kannalta:
Jatkuvan oppimisen identiteetin näkökulmasta SoT-konsepti voi onnistuessaan tuottaa oppijoille hyvin toimivan ja maiden rajat ylittävän keskitetyn ratkaisun, jossa on siemen itsehallittavan identiteetin käytännöille. Tällä hetkellä konsepti ei sisällä toiminnallisuutta käyttäjätietojen välittämiseen kuten alla kuvatut (ks. seuraava luku 4.1.2) edu-ID-ratkaisut, mutta tunnistuspalvelun toimittaisi koulutusorganisaatioista riippumaton SisuID-toimija, jonka hallintomalli ei kirjoitushetkellä ole vielä selvillä.

4.1.2 edu-ID Sveitsissä ja Ruotsissa

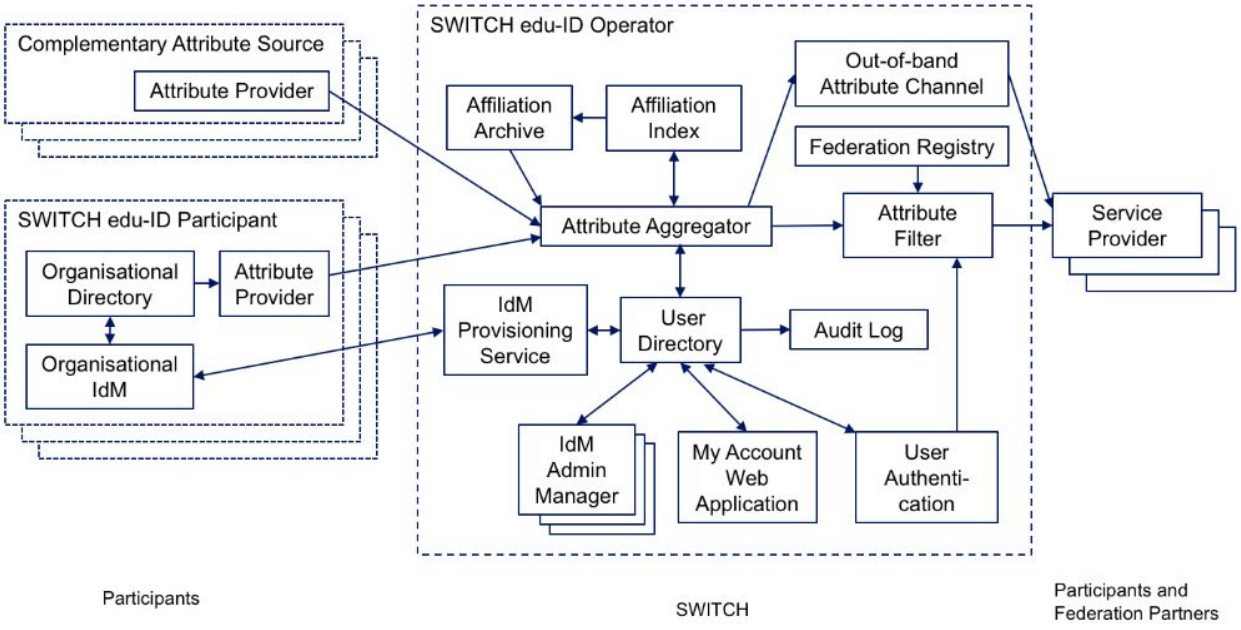
EU-komission rahoittamassa Géant-projektissa on laadittu raportti, jossa analysoidaan ansiokkaasti Sveitsin, Ruotsin ja Italian akateemisten identiteettifederaatioiden toteuttamia käyttäjäkeskeisen identiteetinhallinnan ns. edu-ID-ratkaisuja. Raportissa vedetään yhteen ratkaisujen toteutuserot, ja annetaan suosituksia sekä teknisten toteutustapojen että luottamusverkkojen ja juridisen sääntelyn osalta - osa tämän raportin eduID-suositusehdotuksista periytyy suoraan tästä raportista. Vajavaisuuksina voi nähdä että

GÈANT ei vielä tiedosta ja tarkastele itsehallittavaa identiteettiä keskitetyn federaation ja attribuuttienhallinnan rinnalla, ja keskittyy lähinnä nykyisiin SAML-pohjaisiin eduID-ratkaisuihin. Alla käydään läpi Sveitsin ja Ruotsin eduID-mallit, jotka molemmat täyttävät käyttäjäkeskeisen identiteetinhallinnan perusvaatimukset.

4.1.2.1 Sveitsin SWITCH edu-ID

Koulutusalueen tunnistamisratkaisuja on käyttöönotossa ja jo tuotannossa Sveitsissä ja Ruotsissa. Sveitsin SWITCH edu-ID on projektina aloitettu 2012, ja on käytössä nyt (2018) muutamissa Sveitsin yliopistoissa, kaikki yliopistot pyritään saamaan mukaan integraatioin vuoteen 2020 mennessä. Ratkaisu perustuu keskistettyyn ‘attribuutti-aggregaattoriin’, jota SWITCH IdP-operaattorina hallinnoi, ja osallistuvat yliopistot liitetään siihen sopimuksin ja teknisten federaatioiden avulla - käytännössä liitetyt organisaatiot toimivat vain attribuuttilähteinä affiliaatioon liittyvien attribuuttien osalta. Ydinattribuuttien toimittaminen vastuutetaan käyttäjälle itselleen, ja pysyvä identiteetti luodaan käyttäjän rekisteröinnin yhteydessä. Käytännössä yliopistojen yhteydessä toimivista henkilöistä syntyy SWITCHille yksi laaja edu-ID -käyttäjien rekisteri ja heidän käyttöönsä on tarjolla keskitetty tunnistautumis- ja suostumustenhallinnan palvelu joka aggregoi ja indeksoi käyttäjän kaikki affiliaatiot ja attribuutit edu-ID:hen liitetyiltä attribuuttilähteilltä, joista osa toimii myös paikallisina käyttäjähallintapalveluina. Edu-ID -käyttäjän sovellus on My Account -webbisovellus - verkkopalvelu johon kuuluu käyttäjän attribuuttilompakko ja yksinkertainen suostumustenhallinta, jonka avulla käyttäjä luvittaa valikoidut attribuutit toimitettavaksi niitä pyytäville palveluille.

SWITCH edu-ID:n suunnittelussa on otettu huomioon myös pysyvien tunnisteiden tarjoaminen yliopistovierailijoille, jatko-opiskelijoille, kirjaston käyttäjille jne.. Rekisteröityvän käyttäjän identiteetti varmennetaan lähtökohtaisesti siihen federoidun paikallisen AAI-palvelun kautta tunnistautumalla, mutta myös manuaalinen identiteetin luonti on mahdollista.



Kuva 6. Sveitsin SWITCHin keskitetty edu-ID operaattorimalli[5].

Teknisesti SWITCH edu-ID pohjautuu SAMLiin, sillä kansallinen korvautuva AAI-järjestelmä SWITCHaai on SAMLiin perustuva. Operaattori tukee verkkosivujensa mukaan myös OpenID Connect ja OAuth2 tunnistautumis- ja pääsynhallintateknologioita.

Johtopäätös jatkuvan oppimisen identiteetinhallinnan kannalta:
Sveitsin edu-ID on rakenteeltaan ja hallintamalliltaan ehkä hieman raskas, kansalliseksi ajateltu järjestelmä jota on viety maassa eteenpäin jo 2010-luvun alusta lähtien, jossa oleellista opittavaa on aggregaattorioperaattorin malli ja mahdollisuus luoda joustavasti tunnuksia myös muille kuin oppilaitosten henkilökunnalle ja oppijoille. Mallin puutteita ovat vahvan tunnistamisen irrallisuus eduID-operaattorista, ja toisaalta sillä ei ole näyttäviä mobiilisovelluksen tarjoavia tunnistusvälinekumppaneita (ainakaan saatavilla olevaan kirjalliseen materiaaliin perustuvan analyysin pohjalta).

4.1.2.2 Ruotsin eduID

Kuten Suomessa, myös länsinaapurissa suurin osa koulutusasteiden käyttäjätunnuksista tehdään ilman vahvaa tunnistamista, yleensä sähköpostiosoitteen ja siihen liitetyn salasanan yhdistelmällä. Vahvempi tunnistaminen tarvitaan lähinnä korkeakouluopintoihin kirjautuessa. Ruotsissa on vuodesta 2014 lähtien yliopisto-opiskelijoille ja -alumneille tarjolla eduID -oppijaidentiteettipalvelu - https://eduid.se jonka tarjoavat yhdessä SUNET ja opiskelupaikkojen sähköisestä vastaanottamisesta huolehtiva universityadmissions.se -palvelu. eduID luo

[5] https://projects.switch.ch/eduid/about/architecture/

akateemisille opiskelijoille pysyvän ankkuri-identiteetin ja palvelun jonka avulla opiskelijat luovat paikalliset yliopistotunnukset ja hallinnoivat affiliaatioitaan esimerkiksi yliopiston vaihdon yhteydessä. eduID:n avulla luodaan myös kaksivaiheisen tunnistamisen (engl. 2FA tai MFA) tarjoavat työntekijätunnukset SWAMID-federaatioon kuuluvien yliopistojen henkilökunnalle.

eduID:n pohjatunnisteena toimii aina sähköpostiosoitteen hallinnan todentamiseen perustuva AL1-tasoinen tunnus. Korotetun tunnistustason attribuuteilla varustettu eduID vaaditaan ottaessa vastaan opiskelupaikka ruotsalaisessa yliopistossa, ja useimmiten oppija hankkii AL2-tason vaatimat attribuutit tässä yhteydessä. Hyväksyttyjä menetelmiä korottaa varmennustasoa on muutama, ja ne toimivat tällä hetkellä vain ruotsalaisen henkilötunnuksen (tai väliaikaisen henkilötunnuksen ulkomaalaisopiskelijoiden kohdalla) omaaville henkilöille. Vaihtoehdoista tarkemmin täällä.

eduID:n käyttöönottoa suositellaan sen sivustolla tehtäväksi ensikädessä Verisec AB:n operoiman mobiilisovelluksen, Freja eID:n avulla. iOS- ja Android-versiona tarjolla oleva ilmainen sovellus muistuttaa ruotsissa yleisesti käytössä olevia pankkitunnistussovelluksia, mutta ei tarvitse rekisteröityä pankkitiliä. Freja eID tarjoaa kolme identiteettitasoa: sähköpostiosoitteen hallintaan pohjautuvan varmentamattoman identiteetin, jonka voi korottaa laajennetuksi (“Freja eID Extended”) lisäämällä skannatun kuvan virallisesta tunnisteesta kuten ruotsissa myönnetystä ajokortista tai passista. Vapaaehtoista kasvontunnistustoimintoa (itse otettu kuva käyttäjästä) käytetään Extended-tasolla mm. identiteettivarkauksien ehkäisemisessä.

Kolmannen, eduID:n avulla tehtävän opiskelupaikan vastaanottamisessa tarvittavan vahvimman AL2 -tunnistustason “Freja eID+”:n saa käyttöönsä vierailemalla virallisessa rekisteröintipisteessä (Ruotsissa noin 2000 toimipistettä) jossa henkilö

1) esittää Freja eID -sovelluksen hallintaoikeutensa (kyvykkyyden avata sovellus biometrisellä tunnisteella)
2) antaa rekisteröintipisteen työntekijän tarkistaa nykyisen Freja eID-tason tunnistusattribuuttinsa ja
3) esittää työntekijälle fyysisen viranomaisten myöntämän henkilöllisyysdokumentin kuten ruotsalaisen ajokortin tai passin.

Toimipisteessä paikalla tunnistamiseen käytetään Verisec:in kaupallista ensitunnistamisen työkalua. Tieto myönnetystä vahvasta identiteetistä tulee käyttäjälle sähköpostitse muutamassa tunnissa.

Freja eID -palvelua voi käyttää myös sisäänkirjautumiseen ja transaktioiden vahvistamiseen Nordea tunnuslukusovelluksen tapaan sen käyttöön ottaneissa sähköisissä palveluissa. Käyttöönotto tapahtuu API:n avulla, tarjolla on yksinkertaiset integraatio-ohjeet. Sovellus on Ruotsissa hyväksytty viranomaisten toimesta viralliseksi tunnistautumisvälineeksi (“e-legitimation”) ja kelpaa välineenä myös digitaalisissa julkishallinnon palveluissa. Ruotsiin on

syyskuussa 2018 nimetty uusi viranomainen julkishallinnon digitalisaatiota ajavaksi toimijaksi - DIGG, jonka kautta Freja eID:n käyttömahdollisuus laajenee myös hallinnon palveluissa.

eduID:n tarvitseman AL2-tason voi ottaa käyttöön myös ilman Freja eID-sovellusta, ruotsalaiselle puhelinoperaattorille rekisteröidyn puhelinnumeron ja liittymäsopimuksen olemassaolon varmentamalla (operaattori toimittaa henkilötunnuksen); tämä tapahtuu eduID-palvelun sisään rakennetun operaattoreihin kytketyn kyselyprosessin avulla.

Identiteetinhallinnan ja identiteettiattribuuttien teknologiana eduID käyttää SAML2:ta.

Johtopäätös jatkuvan oppimisen identiteetinhallinnan kannalta:
Ruotsin eduID:n etuja ja mielenkiintoisinta antia ovat käyttöönoton mekanismi heikon tunnistamisen kautta, vahva akateemisen yhteisön sidos ulkopuoliseen, moderniin ja legitiimiin mobiiliin tunnuslompakkoon ja tunnistamisen tason korottamisen menetelmään (Verisec AB:n FrejaID-sovellus ja sovittu tunnistamisprosessi) joka paikallisessa tunnistamisen markkinassa kilpailee melko suoraan Ruotsin vakiintuneen vahvan tunnistamisen verkoston, BankID:n kanssa. FrejaID-sovellus ja siihen liittyvä verkkoportaali on varsin innovatiivinen tunnistamisväline, jolle on tarjolla myös selkeä integraatio-ohjeistus tunnistamisen tarvitsijoille. Verisec AB on kaupallisesta näkökulmasta katsoen investoinut mobiilitunnistamisen palvelun kehittämiseen runsaasti resursseja, ehkä sen seurauksena yritys tekee viimeisten tilikausitietojensa perusteella tappiota.

4.1.3 ORCID iD

ORCID on kansainväisesti toimiva, Yhdysvaltoihin rekisteröity yleishyödyllinen yritys joka tarjoaa tutkijoille oman ilmaisen tutkijatunnisteen (ORCID iD), johon tutkija, tutkimus- ja rahoittajaorganisaatiot voivat liittää tai lukea laajasti erilaisia tietoja tutkijasta kuten tämän vertaisarvioidut julkaisut, affiliaatiot, meritoitumiset, tutkimusaktiiviteetit, -intressit jne. ORCID tarjoaa myös federoitavissa olevan identiteetinhallintaratkaisun ja tietojen auktorisointipalvelun jotka ovat käytettävissä sen jäsenorganisaatioille. Palveluintegraatiot ORCIDiin tapahtuvat hyvin dokumentoitujen OpenID Connect ja OAuth2 -rajapintojen avulla.

Useat tutkimuslaitokset ja yliopistot (myös Suomessa) käyttävät tutkijoiden ORCID-tunnisteita yksikäsitteisesti yksilöivinä tunnisteina esimerkiksi tutkimustietojärjestelmissään, ja ORCID:in tunnistautumispalvelu on federoitu Suomessa Haka-tunnistukseen. Jyväskylän yliopiston tutkijat voivat kirjautua yliopiston työntekijöille tarkoitetuille sivuille ORCID iD:llä. Tutkijatunnisteita ORCIDissa on jo yli 5,5 miljoonaa.

Tunnistuspalvelun ohessa toimivalla auktorisointipalvelulla mahdollistetaan tutkijan luvalla tapahtuva automaattinen julkaisu- ja tutkijan itse hallinnoimien aktiivisuustietojen lukeminen ja kirjoittaminen luotettujen tutkimusorganisaatioiden ja ORCIDin tietovarannon välillä. ORCIDille on kaavailtu vahvaa roolia tulevassa kansallisessa tutkimustietovarannossa (OKM:n projekti, toteutukseen vuosina 2019-2020) jossa sen tehtävä olisi toimia pitkäaikaisen tutkijatunnisteen toimittajana, luotettuna tutkijan omien (itse ylläpitämien) tietojen toimittajana varannon

suuntaan, ja myös tutkimustietovarannon suostumustenhallinnassa tarvittavan tutkijatunnistautumisen (yksilöivän tunnisteen toimittamisen) ratkaisuna.

ORCID iD perustuu teknisesti OpenID Connect:iin ja se tarjoaa toistaiseksi vain sähköpostiosoitteen hallintaan perustuvan alimman tunnistustason (AL0). Vahvempi tunnistustaso (AL2) olisi tarpeen eduID:n tarkempaa käyttäjän tunnistamista vaativiin käyttötapauksiin, kuten opiskelupaikan vastaanottaminen yliopistossa. Lisäksi ORCID iD on lähinnä ylimmän koulutusasteen organisaatioissa toimivien tutkijoiden käytössä, ja sen soveltuvuus muiden asteiden käyttöön ei ole suoraviivaista (attribuuttiavaruus on lähinnä tutkimukseen liittyvä).

Johtopäätös jatkuvan oppimisen identiteetinhallinnan kannalta:
ORCID-tunnisteella on vahva rooli tutkimusmaailmassa, ja toimivat identiteetinhallinta- ja pääsynhallintarajapinnat OpenID Connect ja OAuth2 -ratkaisuihin perustuen. ORCID on looginen linkitettävä identiteetti akateemista uraa tekeville, ja toimii myös tunnistautumispalveluna jos ei tarvita korkeampia tunnistustasoja (tilanne vuonna 2018). Perustunnisteeksi jatkuvan oppimisen ratkaisuihin se ei sovellu. OKM:n tuleva tutkimustietovaranto tulee perustamaan tutkijoiden tunnistamisen ja attribuuttien käytön ORCID-tunnisteisiin. ORCID-tunnistaminen kannattaa joka tapauksessa pyrkiä federoimaan ehdotetun arkkitehtuurimallin tunnistusoperaattorin kanssa.

4.2 Itsehallittavan identiteetin ratkaisut

4.2.1 TrustNet ja FIndy

Business Finland ja useat suomalaisyritykset ovat rahoittaneet verkotettua tutkimushanketta joka tutkii lokakuusta 2017 lähtien Tampereen yliopiston, Oulun yliopiston ja Aalto yliopiston resurssein itsehallittavien identiteettien ja hajautettujen tilikirjojen käyttöä luonnollisten ja oikeushenkilöiden tunnisteiden ja niille myönnettävien attribuuttien (varmennettavien väitteiden ja niistä johdettavien julkituontien) hallinnassa. TrustNet-hanke on tutustunut alueen kehittyviin hajautettujen tilikirjojen teknologioihin kuten Hyperledger Indy (Sovrin) ja uPort, ja hanke on toiminut pohjana ja asiantuntijaresurssina mm. Tiedon, OP:n, Nordean, Asiakastiedon, Veron ja PRH:n yhteisessä lohkoketjujen käyttöön perustuvassa, yritystunnisteisiin liittyvälle palvelupilotille ja Suomen Tilaajavastuun ja Trafin yhteisessä, Trafissa rekisteröityjä ammattilaiskuljettajien ajo-oikeustietoja luvittavan muntiedot.fi -omadata-lompakkopilotille.

DLT-teknologiat ovat kiihkeässä kehitysvaiheessa, kuten myös niihin liittyvät henkilötunnisteiden käsittelysäännöt ja eri toimijakerrosten (tunnisteinfrastruktuuri, eri liiketoiminta-alueiden yhteisesti sovitut luotettujen attribuuttien myöntäjät ja luottamusankkurit) hallinnointiin liittyvät sopimuskäytännöt. EU:n yleinen tietosuoja-asetus asettaa tilikirjojen käytölle erityisrajauksia luonnollisten henkilöiden tunnisteiden osalta, vaikka hajautetut identiteetit (pseudonyymeinä) ovat yleisesti ottaen itsessään ei-henkilöiviä tietoja. Julkiset tilikirjat toimivat selvityksen kirjoitusaikaisen näkemyksen mukaan vain luotettujen oikeushenkilöiden tunnisteiden ja niiden

myöntämien attribuuttien kryptografisena varmennuspaikkana, kun yksittäisten henkilöiden tunnisteet sijaitsevat - tietosuojan maksimoiden - hajautettujen tilikirjojen ulkopuolella. Palvelujen liittäminen henkilön identiteettilompakkoon ja varmennettavien attribuuttien myöntäminen tapahtuu identiteettilompakoiden välisissä vertaisverkkoyhteyksissä. Tilikirjan avulla voidaan varmentaa kryptografisesti julkisen attribuutin myöntäjän identiteetti ja attribuuttitiedon voimassaolo ja väärentämättömyys.

Suomeen on TrustNet-hankkeen tuella muodostumassa 2019 alussa oma hajautettujen tunnisteiden kokeiluinfrastruktuuri (ks. FIndy) jolle luodaan oma hallintomalli ja luottamusverkkosopimukset toistaiseksi korvaamaan Yhdysvaltoihin rekisteröidyn voittoa tavoittelemattoman Sovrin Foundationin hallintomalleja. FIndy-infrastruktuurin avulla on tarkoitus koeponnistaa Suomessa itsehallittavan identiteetin käyttötapauksia eri liiketoiminta- ja public-private-yhteistyön alueilla seuraavien 1-2 vuoden aikana.

Johtopäätös jatkuvan oppimisen identiteetinhallinnan kannalta:
FIndy toimisi Suomessa mahdollisten eduID-attribuuttien myöntäjien tunnisteiden ja attribuuttien voimassaolon varmentamisen alustana kun itsehallittavan identiteetin käytännöt eri osiltaan (teknologia, hallintomallit ja lainsäädäntö) kypsyvät käyttökelpoiselle tasolle. Korkeakoulujen mahdollisen yhteisen eduID-identiteettioperaattorin ja esim. tutkinnot varmentavan KOSKI-palvelun tulisi kunkin liittää itsensä FIndy-verkostoon, toisin sanoen hankkia itselleen hajautetun verkon organisaatiotunnisteet ja toteuttaa omaan IT-järjestelmään tässä ympäristössä tarvittava organisaatiolompakko, jos tällaista palvelua ei tarjota organisaatioille palveluna (“enterprise wallet as a service”, kuten Kanadassa ollaan tekemässä Brittiläisessä Kolumbiassa ja Ontariossa julkishallinnon Suomen PRH:ta vastaavan viraston toimesta). MPASSid voisi teoriassa keskitetyn attribuuttiaggregaattorin roolissa toimia myös toimialan hajautettuja FIndy-organisaatiotunnisteita (koulutusorganisaatioiden Indy-lompakoita) ylläpitävänä palveluna. Lisäksi tulee sopia käytettävistä attribuuteista ja luoda niille varmennettavien väitteiden käytössä vaaditut tietomallit. Näihin kysymyksiin voidaan lähteä hakemaan ratkaisuja asteittain FIndyä hyödyntävillä luottamusverkkokokeiluilla ja luomalla joka tapauksessa ensin vastaavat, keskitetyssä järjestelmässä toimivat OIDC ja SAML -muotoiset attribuutit.

4.2.2 IRMA & Privacy by Design Foundation

Alankomaissa on tarjolla hybridimallinen itsehallittavan identiteetin ratkaisu IRMA (tulee lauseesta “I Reveal My Attributes”), jonka tausta on Radboudin yliopiston tutkimustyössä. Hybridi tarkoittaa tässä yhteydessä teknologian osittaista riippuvuutta keskitetystä PKI-avainten osasten hallintapalvelusta, vaikka käyttäjän IRMA-pohjaidentiteetti ja myönnetyt attribuutit ovat täysin hajautettuina käyttäjien IRMA-sovelluslompakkoihin. Ratkaisun kryptografiset väitteet ja sähköiset allekirjoitukset perustuvat IBM Zürich:in kehittämään Idemix (“Identity Mixer”) -algoritmiin. IRMA:n taustalla on voittoa tavoittelematon säätiö, joka julkaisee ja ylläpitää avoimena lähdekoodina ratkaisun teknologiaa. Säätiö on alkutalvesta 2018 markkinointi- ja operointiyhteistyössä Alankomaiden verkkotunnuspalvelun SIDN:n kanssa, ja IRMA-lompakkoa

kokeillaan identiteetinhallintaratkaisuna mm. Nijmegenin kaupungissa joka myöntää asukkailleen hollannin VRK:lta vastaavan rekisteriviraston identiteettiattribuutit.[67]

Oppimisen identiteettien alueelta eduGain on mukana IRMAn attribuuttimalleihin liittyvissä piloteissa - tunnistautumalla eduGain-tunnuksia käyttävään koulutusorganisaatioon voi lompakkoonsa saada ao. koulutusorganisaation (Suomessa vain Helsingin yliopisto) myöntämät attribuutit - lisätietoja: IRMA eduGain-kokeilu. Julkisesti on saatavilla kaikki kokeiluihin luodut ja IRMA-ekosysteemissä tuetut attribuutit. Myös Alankomaiden Open University ja SURFnet kokeilevat IRMA-identiteettien käyttöä tunnistamisessa.

Johtopäätös jatkuvan oppimisen identiteetinhallinnan kannalta:

IRMA on avoimen lähdekoodin attribuutti- ja zero-knowledge proofeja hyödyntävä ratkaisu, johon liittyy jo eduGain-kokeiluja, myös Helsingin yliopisto Suomesta on mukana tunnistamisen mahdollistavine attribuutteineen. Kokeiluja on käynnissä useita, ja teknologialle on löytynyt arvovaltainen operaattori/ylläpitäjä SIDN. Ratkaisu on lähempänä itsehallittavaa identiteettiä kuin ehdotettu keskitetty arkkitehtuuri tässä dokumentissa, ja ratkaisua kannattaisi koeponnistaa ehkä esim. eduGainin kautta, tai ainakin seurata HY:n kokemuksia. Ehkä myös julkiset attribuuttimallit edu-alueelta kannattaa katselmoida. IRMA-attribuutit ovat ainakin toistaiseksi teknologiasidonnaisia, niiden uudelleenkäyttö muissa hajautetun identiteetin ratkaisuissa on hankalaa.

4.2.3 Migrin Moni-pilotti

Migri ratkaisi paperittomien turvapaikanhakijoiden kotouttamisongelmaa 2016-17 yhdessä Helsingissä toimivan Moni-virtuaalipankkipalveluntarjoajan ja MasterCard-kortteja myöntävän brittiläisen pankin kanssa ns. Moni-pilotissa. Kokeilussa turvapaikanhakijoille saatiin myönnettyä Mastercard prepaid -kortti ja siihen liitetty ominaisuuksiltaan rajoitettu tili, jolle vastaanottoraha siirrettiin sähköisesti normaalin käteismaksun sijaan. Myöhemmin tälle ominaisuuksiltaan edelleen rajoitetulle tilille voitiin maksaa palkkoja ja sitä voitiin käyttää laskunmaksuun.Tämä mahdollisti työpaikan hakemisen, nopean työllistymisen ja palkanmaksun huomattavasti manuaalisia prosesseja tehokkaammin. Migrin omissa ensitunnistamisen prosesseissa toteutettiin ei-sähköinen Know Your Customer (KYC) prosessi jolla pystyttiin suorittamaan MONIN tarvitsema MasterCard-prepaid kortin myöntämiseen riittävä henkilöllisyyden varmennus. Migrillä on henkilötunnuksettomille oma operatiivinen tunniste josta luotiin tässä yhteydessä siihen linkitetty hajautettu tunniste (DID).

Moni-projektin rinnalla tehty “ID 3011”-projekti halusi testata olisiko sama prosessi vietävissä malliksi jossa käytetään itsehallittavan identiteetin tunnisteita, identiteettilompakkoa ja varmennettavia väitteitä. Liiketoiminnan ja teknologian osalta tarvittavat prosessit validoitiin, myös tekniikka itsehallittavan identiteetin osalta: Monilla oli oma organisaation

[6] https://privacybydesign.foundation/issuance-brp/

[7] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/basisregistraties-en-afsprakenstelsels/inhoud-brp/

identiteettilompakko, Migrillä vastaava. Toteutus prototypoitiin nyt jo uudemmalla korvatulla uPort-arkkitehtuurilla. Identiteettien myöntäminen oli hinnoiteltu Ethereumin kryptovaluutassa *gas*:issa. Identiteetin luonti oli silloisessa uPort-ratkaisussa ns. älysopimus (engl. smart contract) joka oli hinnoiteltu Ethereum-kryptovaluutassa.

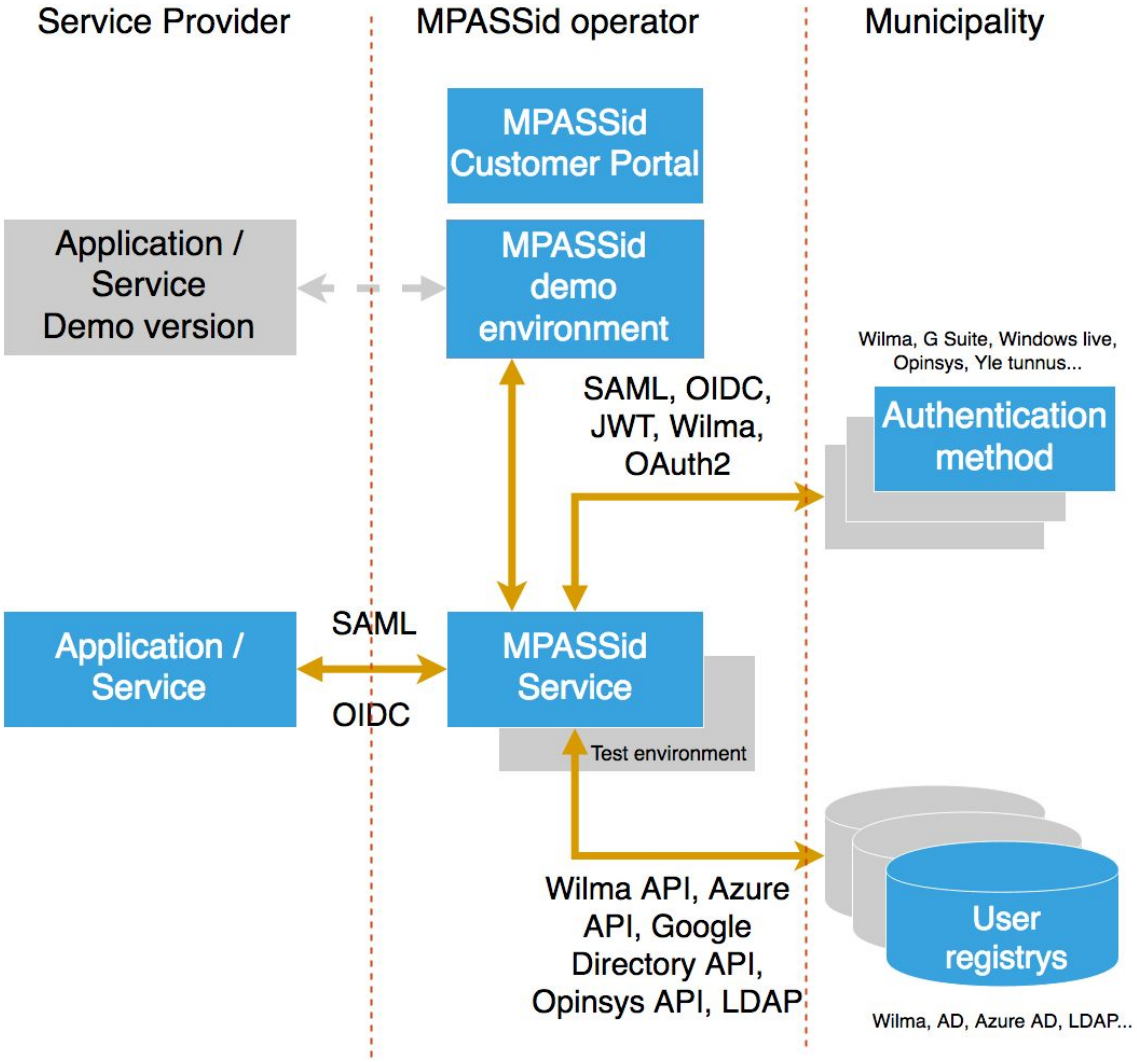
Migrillä ei ole tällä hetkellä aktiivista käynnissä olevaa projektia, jossa edellä kuvattuja kokeiluja vietäisiin tuotantokäyttöön. Asiaa selvitetään kevään 2019 aikana. Migrin nykyisen käytännön mukaan turvapaikanhakijan kolmen kuukauden valvottu maassaolo antaa edellytykset työnteon aloittamiseen ja mm. palkanmaksuun ja verotukseen liittyvien tarvittavien tunnisteiden käyttöönottoon. Migrin varmennettavana väitteenä myönnettävälle identiteettiattribuutille "*voimassaoleva osoite Suomessa*" tarvittaisiin virallisen palvelun status virastossa. "Nollatunnisteen" tuottaminen ja käyttöön sopivan identiteettilompakon käyttöönottoon opastaminen osana maahanmuuttoprosessia olisi liiketoiminnallisesti perusteltavissa oleva palvelu Migrille.

Johtopäätös jatkuvan oppimisen identiteetinhallinnan kannalta:
Migri kannattaa ottaa ehdotetun SisuID-operaattoriratkaisun muodostamiseen aktiivisesti mukaan, erityisesti jos VM/VRK ehdotus henkilötunnuksen uusimisesta päätyy voimakkaammin tunnistamiskäytäntöjä uusivan uuden perustunnisteen, attribuuttipohjaisuuden ja mobiililompakon kannalle. Migrin myöntämien attribuuttien käyttötarve oppimisen yhteydessä tulisi myös varmistaa (maahanmuuttajien kotouttaminen ja palvelu oppimisen alueella).

4.3 Muut

4.3.1 MPASSid

Oppijan polku Suomessa alkaa varhaiskasvatuksesta ja jatkuu oppivelvollisuuden myötä perusopetuksella. Opetuksen tai koulutuksen järjestäjä vastaa oppijoiden ja opettajien sähköisten identiteettien luomisesta henkilörekisteihinsä. Oppijoiden osalta tunnuksen luonti lähtee liikkeelle Väestötietojärjestelmästä (VTJ) opetuksen tai koulutuksen järjestäjien kautta oppilaitoksille lähetettävästä oppivelvollisuuden alkamisesta kertovasta ilmoituksesta. Oppijan tunnisteeksi on valtakunnallisesti vakiintumassa Opetushallituksen KOSKI-palvelun myötä kansallinen oppijanumero, joka tallennetaan kansalliseen rekisteriin, kun henkilö hakee koulutukseen tai kun koulutustoimija siirtää opiskelijoidensa tietoja alla mainittuihin rekistereihin tai tietovarantoihin. Tunnistusratkaisuna toimii perusopetuksessa vuoden 2018 aikana nopeasti yleistynyt MPASSid-tunnistuksenvälityspalvelu, joka pystyy välittämään tunnistetusta oppilaasta käyttäjäattribuutteja, ml. edellä mainitun kansallisen oppijanumeron. Attribuuttien rakenne on SAML2:n nimeämisformaatin mukainen. MPASSid-tunnistusratkaisun arkkitehtuuri on rakenteeltaan keskitetty (Hub&Spoke) luottamusverkosto (identiteettifederaatio), johon opetuksen tai koulutuksen järjestäjät (tyypillisesti kunta) liittyvät kytkemällä oppijoiden ja opettajien tiedot sisältävän henkilörekisterin ja käytetyn tunnistuspalvelun (Wilma, Azure AD, G Suite, tms.).



Kuva 7. MPASSid-ratkaisun tekniset komponentit

Yksikäsitteisenä tunnisteena käytetään MPASSUID:tä, joka on kansallisesti uniikki ID, mutta tunniste vaihtuu käyttäjärekisterin (oppilaitoksen) vaihdon yhteydessä, joten tunniste ei sovellu nykyisessä käyttömuodossaan elinikäiseksi tunnisteeksi.

Johtopäätös jatkuvan oppimisen identiteetinhallinnan kannalta:
eduID-malliin muokattu, keskitetty MPASSid-välityspalvelu välittäisi koulujen tunnistamien käyttäjien attribuutit kolmannen osapuolen tarjoaman pitkäaikaisen tunnisteen tarjoavan tunnistusoperaattorin palvelulle (kuten SisuID) joko SAML2 tai OpenID Connect protokollan avulla MPASSid-tietomallin mukaisesti. Välityspalvelun federointi attribuuttioperaattorin kanssa olisi keino tuoda useat jo olemassa olevat attribuutit ja palvelut suoraan osaksi uutta kehitettävää tunnistuspalvelua.

4.3.2 Henkilötunnuksen uudistaminen

Valtiovarainministeriö käynnisti uuden työryhmän tutkimaan henkilötunnuksen uudistamista elokuussa 2017, ja tutkimuksen väliraportti julkaistiin Lausuntopalvelussa 21.12.2018. Lopulliset tarkennetut ja priorisoidut kehitysehdotukset julkaistaan 2019 aikana.

Työryhmän tehtävänasettelusta:
"Työryhmän tavoitteena on tehdä esitys kansalliseksi toimintamalliksi henkilöiden yksilöimiseen Suomessa ja kuvata viranomaisten rooli henkilöön liittyvien ydintietojen hallinnassa. Tarkoituksena on tuottaa malli, jossa henkilön yksilöivä tunnus ja siihen liittyvät tiedot voidaan hallita erillisinä sekä toiminnallisesti että juridisesti...nykyisen henkilötunnuksen ongelmakohtia ovat muun muassa tunnuksen myöntämisen toimivalta, tunnuksen myöntäminen kaikille Suomeen tuleville henkilöille, henkilön tunnistaminen tunnuksen antamisen yhteydessä, biometristen tunnisteiden liittäminen, tietojen hallintaprosessi sekä tunnuksen käyttäminen järjestelmien välillä henkilön identifioimiseen...tavoitteena on...edistää henkilöön liittyvien rekisteritietojen hajautettua hallintaa ja käyttöä tietoa kysytään vain kerran –periaatteen mukaisesti, edistää henkilön nykyistä laajempaa mahdollisuutta itseensä liittyvien tietojen hallintaan ja hyödyntämiseen myös yksityisen sektorin palveluissa, sekä tietoturvallisten menetelmien käyttämistä henkilön identifioimisessa."

Asiantuntijahaastattelujen ja työryhmän väliraportin perusteella lopullista ehdotusta kolmesta mahdollisesta etenemispolusta ei vielä ole priorisoitu. Attribuuttipohjainen tunnistaminen on ehdotuksen kahden uudistavamman toteutusehdotuksen ytimessä, ja siihen voitaisiin siirtyä hallitusti aluksi keskitetyn tunnistushallinnan (kappale 7.3) avulla, ja myöhemmin mahdollisesti itsehallittavaan identiteettiin ja identiteettilompakkoratkaisuihin nojautuen (kappale 7.4).

Työryhmältä odotetaan 2019 aikana lopullisen toteutusmalliehdotuksen lisäksi lainsäädäntöluonnosta jossa kirjataan tarvittavat lakimuutokset ehdotuksen toteuttamisen mahdollistamiseksi.

Johtopäätös jatkuvan oppimisen identiteetinhallinnan kannalta:
Työryhmän lopullinen ehdotus on ehdottoman oleellinen mahdollisen eduID-ratkaisun kehittämisen näkökulmasta. Olettaen että keskitetty tunnistushallinta saisi työryhmän puollon, ei ole järkevää lähteä koulutusalueen oman tunnistuspalvelun kehittämiseen vaan resurssit kannattaa sitoa olemassa olevien palvelujen integroimiseksi uuden järjestelmän osaksi.

4.3.3 EU Blockchain Partnership Agreement & eSSIF

EU:ssa on Saksan vetämänä lähdössä liikkeelle laajempi itsehallittavaan identiteettiin pohjautuva eGovernment-hanke, jossa tavoitellaan yhteistä eri itsehallittavien identitteettien yhteensopivuuden mahdollistavaa, eIDAS-tunnistamisen kanssa juridisesti sovitettua SSI-infrastruktuuria useampien jäsenmaiden kesken. Viitekehyksenä on EU Blockchain Partnership -sopimus jonka useat EU:n jäsenvaltiot ja Norja solmivat huhtikuussa 2018, ja hanke olisi Horizon2020 tutkimus- ja tuotekehityshanke. Suomea edustaa EBP-ryhmässä Kimmo Mäkinen Valtiovarainministeriöstä, se pitää kokouksia Brysselissä kerran kuukaudessa. Suomi on ilmaissut halukkuutensa osallistua eSSIF-hanketyön valmisteluun talven 2019 aikana, itse Horizon 2020 -hanke alkaisi vuoden 2019 loppupuolella jos DG Connect myöntää rahoituksen. Mukaan ovat alustavasti lähdössä Saksa, Alankomaat, Belgia, Italia, Espanja, Slovenia, Puola, Viro ja Kreikka. Ruotsi osallistui aloituskokoukseen kuten Suomi mutta todennäköisimmin jää observaattorin asemaan. DG Connect on viimeisten tietojen mukaan yhdistämässä hankkeen hakua ja lopullista rahoitusta toisen haussa olevan eGovernment-kehitysohjelman, ns. OOP:n (Only Once Principle) konsortion kanssa, ja kolmivuotisen ohjelman kokonaisrahoitus voi olla 8 MEUR.

Johtopäätös jatkuvan oppimisen identiteetinhallinnan kannalta:
Mielenkiintoinen kehyshanke piloteille itsehallittavan identiteetin malleilla, ja tullee aktiivisesti ratkaisemaan lainsäädäntöön ja teknologiakysymyksiin kuten yhteentoimivuuteen liittyviä kysymyksiä EU:n alueella jos hanke saa rahoituksen (tämä tiedetään syksyllä 2019). eSSIF-hankkeen rinnalla on jo olemassa käynnistyvä DIPLOMA-hanke (“Network of trust for education a.k.a. Cross-border Blockchain for Diploma Data in the EU”), jossa useampi EU-maa (Belgia, Norja, Hollanti, Italia, Malta, Ranska & Kroatia) aikoo pilotoida tutkintotietojen välittämistä itsehallittavan identiteetin mekanismeilla. Tämä kokeilu on tuotu CSC:n tietoon syksyllä 2018, mutta osallistumiseen ei liene mahdollisuuksia. Kokeilun tulokset kannattaa kuulla jos Suomella on jatkossa pysyvämpi yhteys eSSIF:n ja EU Blockchain Partnership-sidoksen (VM/Kela edustajat) tai FIndy-infrastruktuuria aikanaan pyörittävän organisaation kautta.

4.3.4 EU Fintech/remote KYC työryhmä

Euroopan komissiossa on asiakkaan sähköistä henkilöllisyyttä ja asiakastunnistamista asiantuntijaryhmä “Expert Group on electronic identification and remote Know-Your-Customer processes**”**, lyhyemmin eID/KYC asiantuntijaryhmä. Euroopan komissiossa pidettiin ryhmän fasilitoimana syyskuun 2018 lopulla kuulemistilaisuus tarjolla olevista asiakkaan tunnistamisesta säädetyn EU-lainsäädännön vaatimukset täyttävistä identiteetinhallinnan tekninistä ratkaisuista. Tärkeimmät esitetyt ratkaisuvaihtoehdot olivat Sovrin/Indy tilikirjaan pohjautuva itsehallittava identiteetti ja keskitetty, eIDAS-kokonaisuudessakin jo tuettu OpenID Connect. Työryhmän työn pohjalta on nähtävästi syntymässä kilpaileva H2020-ehdotus maaliskuun 19. 2019 sulkeutuvaan

hakuun “New forms of delivering public goods and inclusive public services”[8] johon myös eSSIF-konsortio valmistelee hakemusta.

4.3.5 #AuroraAI TP2. Kiinni työelämässä osaamisen kehittämisen avulla

Valtiovarainministeriö käynnisti kansallisen tekoälyohjelma Auroran esiselvityksen 17.9.2018, esiselvitys valmistuu 28.2.2019. Se on osa Tekoälyaika Suomessa -raportin ehdotuksia. Esiselvitys vauhdittaa julkisen hallinnon siirtymistä tekoälyaikaan ja luo kokeiluversion tekoälyjen/autonomisten sovellusten muodostamasta hajautetusta palveluverkko Aurorasta, jolla luodaan edellytyksiä yhteiskunnan palvelujen ihmiskeskeiselle ja ennakointikykyiselle tarjoamiselle. Monitoimijaisessa kokeilussa tehdään töitä yksilön hyväksi. Palvelumuotoilu, käyttäjien kuuntelu ja yhdessä ideointi, sekä avoimuuden ja tiedon jakamisen periaatteet viitoittavat laajan verkoston työskentelyä. Kokeilu toteutetaan julkisen ja yksityisen sektorin toimijoiden tiiviissä yhteistyössä.

Yksilön ehdoilla data hyötykäyttöön - kohti digiminää ja personoitua palvelutarjontaa

Auroran Kiinni työelämässä osaamisen kehittymisen avulla -työpaketissa kehitettiin ja kokeiltiin tapoja tekoälyn hyödyntämiseen jatkuvan oppimisen ja työllisyyden kontekstissa, huomioiden vastuullisuus ja eettiset näkökulmat. Kokeilussa selvitettiin, miten Aurora-palveluverkko löydetään ja miten siihen liitytään, miten osaamista, tavoitteita ja kiinnostusta kartoitetaan, miten käyttäjä saa tietoa oman osaamisen kehittämiseksi tai työllistymiseksi.

Aluksi palveluverkko voisi auttaa käyttäjää luomaan digiminän/digikaksosen profiiliin ja tuomaan dataa eri tietolähteistä (julkiset ja yksityiset) osaksi profiilia sekä jäsentämään käyttäjän nykyosaamista ja tavoitteita. Profiilidatan, tulevaisuus-, ennakointi- sekä työmarkkinatiedon louhinnan sekä matchauksen avulla henkilö voi saada tietoa hänelle soveltuvasta palvelutarjonnasta mm. suosituksia soveltuvista osaamisen kehittämis- ja työmahdollisuuksista nykyisessä elämäntilanteessa sekä ohjausta ja valmennusta asiantuntijalta.

Kokeiluun kuuluivat myös selvitykset palveluverkkoon rekisteröitymiseen, tunnistautumiseen, MyDatan käyttöön ja suostumusten hallintaan sekä käyttäjän ja palvelutarjoajien saamaan arvon mittaamiseen liittyen. Tämä jatkuvan oppimisen identiteetinhallinta -selvitys on osa AuroraAI:n toimenpiteitä. Pitkällä aikavälillä personoitu palvelutarjonta voi mahdollisesti toimia ratkaisuna kohtaanto-ongelmaan muuttuvien osaamistarpeiden näkökulmasta.

[8] Linkki Horizon 2020 hakuun: https://bit.ly/2FLnI14

4.3.6 Suomen Tilaajavastuun MyData-lompakko

Suomen tilaajavastuu kehittää TrustNet-hankkeen puitteissa Trafin kanssa pilotoitavaa, avoimena lähdekoodina julkaistavaa omadata-operaattoripalvelua. Toteutuksen arkkitehtuuri tulee perustumaan sekä keskitetyn identiteetin- ja pääsynhallinnan (OpenID Connect & OAuth2) että hajautettujen identiteettien (Hyperledger Indy) käyttöön.

Kuva 8. Tilaajavastuun ja Trafin omadatapilotin käyttötapaus.

Ensimmäinen pilotointikohde Tilaajavastuun suostumustenhallinta- ja identiteettilompakolle on Trafin rekisteristä rajapinnan kautta tarkistettavien ajo-oikeustietojen toimittaminen Tilaajavastuun omalle Taito-palvelulle Valtti-lompakon välityksellä. Tilaajavastuu toimii pilotissa omadata-operaattorina eli käyttäjä hallinnoi tietojensa siirtoon liittyvät suostumukset palvelussa, jonka toteutus näkyy kuvan 8 vasemmassa yläkulmassa käyttäjän puhelimessa toimivana ‘lupalompakkona’ (Valttikortti). Lompakon toteutuksesta reaktiivisena, mobiilikäyttöön soveltuvana verkkosovelluksena on julkaistu elokuussa 2018 käyttöliittymätasoinen luonnos ja esitysmateriaalit.

Luonnollisten henkilöiden identiteetit ja suostumukset hallinnoidaan omadata-operaattorin keskitetyissä rekistereissä, mutta suostumuksiin ja tiedonsiirtoon liitetyt lähde- ja hyödyntäjäpalvelut tunnistetaan järjestelmässä perustuen niille myönnettäviin julkisiin

hajautettuihin tunnisteisiin (DID:eihin). Suunnitelman mukaan yritysten hajautetut tunnisteet talletetaan pilotissa esimerkiksi FIndyn tarjoamaan julkiseen tilikirjaan.

Kenttäkäyttöön pilottia odotetaan 2019 ensimmäisellä neljänneksellä ja sen kesto on suunniteltu elokuun 2019 loppuun. Pilottiin osallistuu ammattikuljettajia (max. 200) ja muutama Taito-rekisterin kautta saatavia ajo-oikeustietoja hyödyntävä rakennusalan yritys.

4.3.7 KOSKI-palvelu ja OmaData-pilotti

Opetushallitus vastaa ns. KOSKI-lain (884/2017) määräämällä tavalla palvelusta, joka kokoaa yhteen kootusti ja yhteismitallisesti tiedot mm. opintosuorituksista ja opiskeluoikeuksista eri koulutusasteilla. Laissa määrätään myös opinto- ja tutkintotietojen luovutuspalvelusta, josta luovutetaan 1) perus- ja toisen asteen ja 2) korkea-asteen tietoja sekä 3) opiskelijavalintarekisterin ja 4) ylioppilastutkintorekisterin tietoja. Myöhemmin palvelun osaksi tulee myös varhaiskasvatuksen tietovaranto, josta määrätään varhaiskasvatuslaissa 540/2018. Osana KOSKI-palvelua lanseerattiin vuoden 2018 aikana kansalaisten palvelunäkymä, joka näyttää vahvasti tunnistautuneille henkilöille koulutushistoriatiedot yhden palvelun kautta ja mahdollistaa tietojen välittämisen edelleen secure link:n avulla. Palvelu tarjoaa myös OmaDataperiaatteiden mukaista koulutustietojen toisiokäyttöä ensimmäisenä julkishallinnon palveluna ns. suostumuksenhallintapalvelun kautta. OmaData-pilottina rakennetun palvelun avulla henkilö voi luovuttaa tietonsa esim. yksityisille palveluntarjoajille.

KOSKI-laissa määrätään myös oppijanumerorekisteristä, josta vastaa Opetushallitus. Oppijanumero on henkilölle annettava pysyvä yksilöintiin tarkoitettu tunnus, joka muodostetaan, kun henkilöstä tallennetaan ensimmäistä kertaa KOSKI-laissa määriteltyjä tietoja. Käytännössä oppijanumero muodostetaan siinä vaiheessa, kun henkilö hakee koulutukseen Opintopolku-palvelussa. Tämän lisäksi tietoja käsittelevät organisaatiot (esim. korkeakoulut) voivat lain määräämällä tavalla hakea oppijanumeroita palvelusta. Ellei henkilöllä jo ole oppijanumeroa, se luodaan palvelussa. Oppijanumeron käytön laajenemista hidastaa se, että henkilötunnuksettomien henkilöiden tunnistaminen tapahtuu virkailijatyönä. Lisäksi henkilötunnuksettomalle henkilölle voi muodostua useita oppijanumeroita, jotka täytyy manuaalisesti yhdistää samalle henkilölle niin, että yksi tunnuksista on ensisijainen. Ongelmat johtuvat nykyisen henkilötunnuksen myöntämiseen liittyvistä rajoitteista, joihin VM:n työryhmä on parhaillaan etsimässä ratkaisuja (ks. luku 4.3.2).

4.4 Yhteenvetotaulukko

Arkkitehtuuriehdotuksen pohjaksi on alla vertailtu kolmea toteutuspolkuvaihtoehtoa, joista kaksi pohjautuu keskitettyyn identiteetinhallintajärjestelmään ja yksi hajautettujen tilikirjojen soveltamiseen identiteetinhallinnassa. Ensimmäinen olisi Ruotsin tai Sveitsin mallisen kansallisen eduID-operaattorin perustaminen jatkuvan oppimisen organisaatioiden tarpeisiin, toinen Sandbox of Trust -identiteetinhallintamallin soveltaminen eduID:n tarpeisiin ja kolmas

puhdas itsehallittavan identiteetin malli toteutettuna esimerkiksi Indy-ledgerin ja kansallisen tai kansainvälisen governanssikehyksen (hallintomallin ja sopimusten) alla.

Kriteeri	“Kansallinen eduID”	SisuID jossa osana eduID (Sandbox of Trust)	Itsehallittava identiteetti (Sovrin/Indy)
Kansainvälinen yhteentoimivuus olemassa olevien akateemisten tunnistusratkaisujen kanssa (kansalliset federaatiot, ORCID-id, eduID)	Toteutettavissa noudattamalla GÉANT ja REFEDS yhteisöjen suosituksia	Toteutettavissa noudattamalla GÉANT ja REFEDS yhteisöjen suosituksia eduID-atrribuuttien ja hallintamallin osalla	? (ensimmäiset kokeilut EU:ssa 2019-2021)
Kansainvälinen yhteentoimivuus kansallisten ja EU-tason (EIDAS) kansalaisen tunnistusratkaisujen kanssa	Lähtökohtaisesti eri federaatio kuin eIDAS-identiteetin myöntäjien verkosto. Italian (GARR) tuleva malli ehkä toimii.	Tehtävissä jos SisuID ensitunnistaminen sertifioituu tasolle 2 (substantial)	Auki. Ensimmäiset EU-hankkeet eIDAS-pohjaisesta SSI-identiteetistä 2019-2021
Oppijatunnisteen pysyvyys (50-80 vuoden ajaksi)	Julkinen hallinto sitoutettava pitkäaikaiseksi operaattoriksi	Tunnistamisosuus-kunta, jossa valtio yksi osakas (auki)	?
Tunnisteiden korreloimattomuus	Vahva korrelaatio (operaattori)	Operaattori pystyy korreloimaan	Sama tunniste eri palveluissa vain käyttäjän niin halutessa
Vikasietoisuus	Operaattori on single-point-of-failure DDoS?	Operaattori on single-point-of-failure DDoS?	Hajautettu Käyttäjille tarvitaan yksinkertainen lompakon varmuuskopiointi-mekanismi
Teknologian kypsyystaso	Vakiintunut (2005)	Tulossa käyttöön (2011)	Kypsymätön
Teknologian kustannukset	Oma operaattori	Osuuskuntakustan-nukset / vuosi	Agentti/lompakko/ attribuuttitoteutukset

			organisaatioissa ja mobiililompakko
Teknologian kehitystyökalut, ekosysteemivahvuudet	Avointa lähdekoodia Vakiintuneet työkalut SAML käytössä eduID-järjestelmissä Ei toimi mobiiliympäristöissä	Avointa lähdekoodia OpenID Connect:in rooli kasvussa (Web+Mobile)	Avointa lähdekoodia Työkalut vasta kehittymässä Hyvin hajautettu kehittäjien ekosysteemi