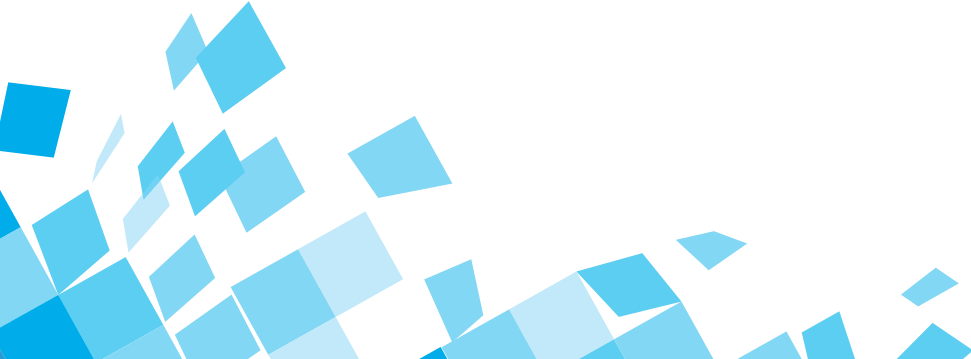
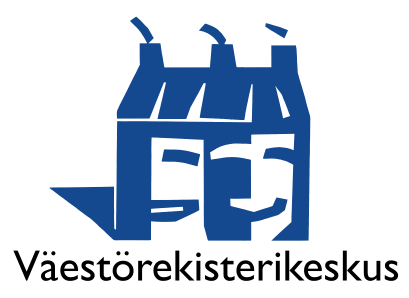
|  |
| --- |
|  |
| **SUOSTUMUSPERUSTEINEN HENKILÖTIETOJEN HALLINTA** |
|  |
| Visio suostumusperusteisen henkilötietojen hallinnan tavoitetilasta julkisessa hallinnossa |
| **TYÖPAJAVERSIO 17.1.2018** |



|  |  |
| --- | --- |
| DOKUMENTINHALLINTA | |
| Omistaja | Väestörekisterikeskus |
| Laatinut | Harri Honko, Mika Honkanen, Jaana Nevalainen, Anu Ylä-Pietilä, Riitta Partala (skenaariot), Suvi Remes |
| Tarkastanut | Mika Honkanen, Suvi Remes ja Jaana Nevalainen |
| Hyväksynyt |  |

Sisällysluettelo

[**Johdanto**](#_kjncxm270fk6) **4**

[Tämän dokumentin tarkoitus](#_ndb6njczev64) 5

[Dokumentin kohderyhmä](#_fhtanp2ighhi) 6

[Rajaukset ja reunaehdot](#_jc8wgmwn7b0w) 7

[Asiakirjassa käytetty terminologia ja sanasto](#_m6xporubxl0b) 7

[**Periaatetason arkkitehtuurikuvaukset**](#_xh53s3xc16bb) **11**

[Omadatan käyttötarpeet julkishallinnossa, nykytilanne ja (liike)toimintaympäristö](#_uijdn96y1dbz) 12

[Suostumus](#_jtuatpp7zjld) 12

[Käsittelystä notifiointi](#_n1ggv6rl2jfh) 13

[Kiellot ja käsittelyn vastustaminen](#_5mwds1n8s9jv) 14

[Suostumusten siirrettävyys](#_7b9euod2xyii) 14

**Nykytila kansallisen palveluarkkitehtuurin ja tiedon hallinnan näkökulmasta 14**

[Lainsäädännöllistä selvitystä vaativat asiat](#_30j0zll) 16

[**Toiminnallinen omadata-arkkitehtuuri**](#_avyhaf3q5307) **20**

[Vaiheessa 1 identifioidut omadata-käyttötapaukset](#_9nfkpfutf0qe) 24

[Koulutus- ja opiskelutietojen hyödyntäminen](#_19yyzx1ig5d8) 25

[Verotustietojen hyödyntäminen lainahakemuksessa](#_98r0wjbd4x37) 26

[Minun Helsinki (Helsinki)](#_qchtcv2u791f) 27

[Ajoneuvon vertaisvuokrauspalvelu (Trafi)](#_896172v7a4b0) 28

[Vaiheen 2 edistyneet käyttötapaukset](#_59x56z4d4s82) 28

[Suostumuksen antaminen ja hallinta Hyödyntäjäpalvelussa](#_s2zqsertj7eq) 29

[Notifiointi ja henkilötietojen käsittelyn läpinäkyvyys](#_5hj1nsd32zlg) 29

[Henkilötietojen käsittelyn vastustaminen](#_tz4vy3jmnzy9) 30

[**Tietoarkkitehtuuri**](#_kw1vd3z3ctz5) **32**

[Käsitemalli](#_1ahul23geyw7) 32

[Omadataan liittyvät tiedot ja tietomallit](#_r48xz7q6y74j) 34

[Loogiset tietovarannot](#_vb4zxav39xim) 37

[Tietovirrat](#_ybedwrn5dis9) 37

[**Tietojärjestelmäarkkitehtuuri**](#_u4cipxbxnizu) **39**

[Suostumustenhallintapalvelu](#_rjjm5afj75q9) 39

[Suomi.fi:n suostumustenhallinta-infrastruktuuripalveluskenaariot (Vaihe 1)](#_4a6i65y937hb) 40

[Keskitetty Suomi.fi-suostumustenhallinta](#_v4xjlaefpof6) 40

[Hajautettu sektorikohtainen suostumustenhallinta](#_uojbdf6b946z) 41

[Hybridimallinen suostumustenhallinta](#_r9g4swn3pm3d) 43

[Avainvaatimukset](#_pzxzashhemob) 44

[Suostumustenhallintapalvelun komponentit](#_unmaor8ljjqc) 46

[Hallintalogiikka](#_e0739ec1nofn) 46

[Hallintanäkymä](#_zalqtxax33h1) 47

[Rajapinta-asiakas](#_hiskf0khakfu) 48

[Suostumustallenne](#_wegs7ge7z0rm) 49

[Suostumuksenhallinnan ohjelmistorajapinnat (APIt)](#_2kgf2wlyl4hy) 53

[Suostumustenhallinnan tavoitetila (Vaihe 2)](#_1r8tz0h2d1jc) 56

[Yhteinen palvelu julkishallinnon palvelukartalla](#_9zgm643czspl) 56

[Luvitusnäkymät luotetuissa Hyödyntäjäpalveluissa](#_m3qcmltklm4j) 56

[Identiteetin luottamustasot ja suostumus eri tiedoille](#_9in26d50ds0s) 57

[Hajautetut tilikirjateknologiat suostumustenhallinnassa](#_a3o0bmhuvo3i) 58

[Kansalaisen uusi digitaalinen tunniste](#_5djm8pnpmju1) 61

70

[**Liitteet**](#_nlra6ggqiniu) **71**

Liite 1 - Luonnosteltuja OPH:n, Veron, Helsingin kaupungin ja Trafin omadata-käyttötapauksia

[Liite 2 - Suostumuskyselyn prosessikaavio (PDF originaali)](#_aaj1jntiiotb)

[Liite 3 - Suostumuspyynnön prosessikaavio (PDF originaali)](#_47cl6nfjci8v)

Suostumusperusteinen henkilötiedon hallinta

# Johdanto

Informaation luoma arvo kasvaa, mitä enemmän sitä käytetään. Olemassa olevasta informaatiosta saa enemmän arvoa irti, jos sitä hyödynnetään enemmän useamman toimijan johdosta. Tästä syystä julkisen hallinnon hallinnoimat tietovarannot voivat toimia arvokkaana resurssina koko ympäröivälle yhteiskunnalle nykyistä laajemmin ja erilaisimmilla tavoilla. Kokonaisvaltainen informaation hallinta voi jakaa julkisen hallinnon hallinnoiman tiedon karkeasti kolmeen osaan: avoimeen dataan, omadataan ja suljettuun dataan.

Avoimen datan määritellään olevan tietoa, jota voi käyttää ja edelleen jakaa vapaasti; usein ainoastaan sillä ehdolla, että sen alkuperäinen lähde mainitaan (katso esim. [Creative Commons 4 by](https://creativecommons.org/licenses/by/4.0/) tai sen pohjalta tehty [JHS-189](http://www.jhs-suositukset.fi/suomi/jhs189)). Julkisessa hallinnossa avointa dataa ovat esimerkiksi kartat, lainsäädäntö, sääennustukset ja kansalliset tilastot. Avoin data ei voi sisältää mitään salassa pidettäviä tietoja tai henkilötietoja. Henkilötiedoilla henkilötietolain mukaan tarkoitetaan kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa koskeviksi. Myös henkilötietoa voidaan antaa koneluettavana henkilön itsensä edelleen käytettäväksi ja hallinnoimiseksi, ja sitä voidaan hallinnoida esimerkiksi suostumuspohjaisesti. Vähimmäiskriteeri sille, että jokin henkilötieto lasketaan omadataksi, on se, että yksilöillä on laillinen oikeus ja tekninen mahdollisuus uudelleenkäyttää ja jakaa tietoaan haluamallaan tavalla. Kolmas informaation tyyppi on suljettu data, jota voi käsitellä vain tietty toimija tietyin perustein.

Tämä asiakirja keskittyy kuvaamaan suostumuspohjaista koneluettavien henkilötietojen hallintaa. Tähän luokkaan kuuluvaa informaatiota on arvioitu olevan merkittävä määrä julkisessa hallinnossa. Toisaalta sen käsittelyyn liittyy myös rajoitteita. Käsittelyn tulee huomioida esimerkiksi yksityisyyden suojan asettamat vaatimukset. Viiden maailman arvokkaimman yrityksen liiketoimintamallit perustuvat pitkälti henkilötietojen keräämiselle ja hyödyntämiselle[[1]](#footnote-0). Esimerkiksi Google (Alphabet) tietää, mitä ihmiset etsivät, Facebook tietää mitä he jakavat ja ketä heidän lähipiiriin kuuluu ja Amazon tietää, mitä mitä he ostavat ja suunnittelevat ostavansa. Monet internetin palveluista on rahallisesti tarkasteltuna maksuttomia, mutta asiakkaat maksavat niiden käytöstä jakamalla omia henkilötietojaan yhä enemmän.

Suostumuspohjainen koneluettavien henkilötietojen hallinta laajentaa – mutta ei korvaa – julkisen hallinnon säädösperusteista henkilötietojen hallintaa. Se siis luo uusia mahdollisuuksia nykyisten toimintatapojen rinnalle. Kokonaisvaltainen tapa lähestyä asiaa voi merkittävästi kehittää ja uudistaa yhteiskunnan tapaa toimia ja palveluita. Toisaalta se mahdollistaa sähköisessä muodossa toimivat tietovirrat, joiden avulla monia asioita voidaan toteuttaa nykyistä tehokkaammin.

## Tämän dokumentin tarkoitus

Tämä asiakirja on suunnitteluasiakirja, jonka pohjalta on tavoite laatia viitearkkitehtuuri henkilökeskeiselle tiedon hallinnalle, ns. omadatan (ks. [terminologia](#_m6xporubxl0b)) käsittelylle julkishallinnossa.

Asiakirja käsittelee erikseen lyhyen tähtäimen, nykyratkaisuihin (Suomi.fi palvelut nykymuodossaan) pohjautuvan omadata-arkkitehtuuriehdotuksen, jolla on tarkoitus mahdollistaa julkisen hallinnon omadata-palvelujen pilotointi (1. vaihe), ja toisaalta kuvaa visioidun tavoitetilan, jossa omadataa käyttävien palvelujen kehittäminen ja käyttö hallinnossa on integraalinen osa päivittäistä toimintaa (2. vaihe). Dokumentin kuvissa ja teksteissä kuvattu Suomi.fi-palveluiden käyttö on tavoitetila, jonka konkreettinen toteutus hankkeistetaan erikseen. Hankkeistamissuunnitelmia ja ehdotuksia tarkennetaan myöhemmin vuoden 2018 aikana ensimmäisistä omadata-palvelukokeiluista kertyvien oppien kautta.

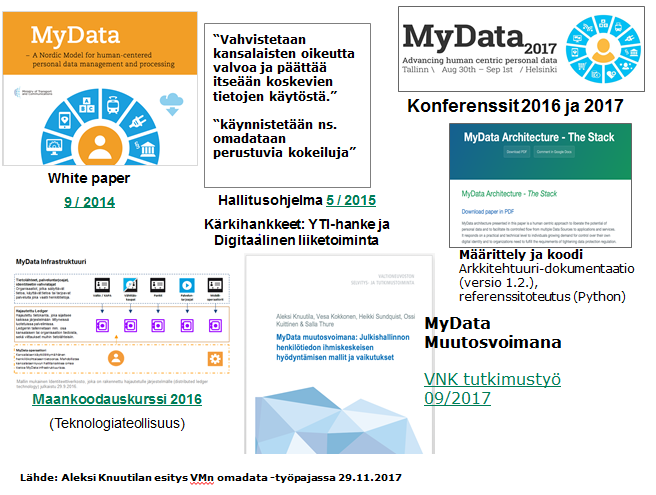
Kokeilujen kautta toteutettavan ensimmäisen vaiheen konseptoiduista arkkitehtuuriratkaisuista suostumustenhallintaan keskustellaan kappaleessa [Suomi.fi:n omadata-infrastruktuuripalvelu](#_4a6i65y937hb). Kokeilujen avulla luodaan palveluiden lisäksi yhteisiä toimintatapoja tiedon hallintaan.

Vaiheen 2 tavoitetilan tieto- ja tietojärjestelmäarkkitehtuurien osiot käsittelevät tukipalveluiden ja suostumustenhallinnan tarvitsemat teknologia- ja arkkitehtuuriratkaisut laajemmin. Asiakirja ottaa laajemman ohjelmistoteknologia- ja tietojärjestelmäkehyksen lisäksi kantaa myös omadatapalveluiden kannalta oleelliseen julkisen hallinnon sähköisen palvelujen ohjelmointirajapintojen (API:en) hallintaan, ja organisaatioiden omille tai alihankkijoina toimiville palvelukehittäjille tarkoitettujen julkishallinnon yhteisten digitaalisten tukipalvelujen muutostarpeisiin. Jatkotyössä tarkennettavan viitearkkitehtuurin realisointitoimenpiteet jakautuvat useille julkisen hallinnon viitearkkitehtuurin osien IT-kehityshankkeille ja erityisesti vaiheen 2 toimenpiteet vaativat strategisia priorisointeja.

Suuri osa omadata-palvelujen mahdollistamiseksi jatkokehitystä tarvitsevista, olemassa olevista tietojärjestelmistä tai yhteisistä tukipalveluista on asiakirjan laatimishetkellä Väestörekisterikes-  
kuksen hallinnoimia, ja ne ovat eri kehitysvaiheissa.

Arkkitehtuurityö, siihen liittyvät selvitykset, työpajat ja kuulemiset, on osa *Yhteinen tiedon hallinta* -kärkihankkeen[[2]](#footnote-1) toteutusta. Hankkeen toimenpiteiden tavoitteena on luoda toimintarakenteet ja perusinfrastruktuuri tehokkaalle yhteiselle tiedon hallinnalle julkisessa hallinnossa. Henkilökeskeisen tiedon hallinnan kehittämistoimien tavoitteena on, että rekisteröity voi käyttää ja hyödyntää omia julkisen hallinnon hänestä tallentamia tietoja omadata-periaatteita soveltaen. Lisäksi tavoitteena on vahvistaa julkisen hallinnon kykyä toimia hyvänä ja esimerkillisenä omadata-toimijana ja toimintaperiaatteen mahdollistajana. Omadatan toteutuksessa on kyse myös siitä, miten viranomainen ja henkilöasiakas toimivat joustavassa vuorovaikutuksessa.

Dokumenttia laadittaessa on mahdollisuuksien mukaan hyödynnettyjä muita jo tehtyjä selvityksiä ja tutkimuksia. Kuvaan 1 on koottu lyhyesti keskeisiä teemaan liittyviä selvityksiä, tapahtumia ja tuotoksia.



Kuva 1. Omadataan (myös MyData) liittyviä selvityksiä, tilaisuuksia ja tuotoksia.

## Dokumentin kohderyhmä

Tämä henkilötiedon suostumusperusteisen hallinnan arkkitehtuurikuvaus on tarkoitettu julkisen hallinnon toimijoille, jotka ylläpitävät kansalaisten henkilötietoja sisältäviä rekistereitä, ja pohtivat tietojen laajempaa hyödyntämistä sitä omadataksi avaamalla. Hyödyntäjät ovat useimmiten tietoa tarvitsevia loppuasiakaspalvelujen kehittäjäorganisaatioita ja niiden yhteistyökumppaneita, ja voivat olla myös yksityisen sektorin toimijoita. Asiakirja toimii myös päätöksenteon tukena omadataan liittyvän IT-arkkitehtuurin, ohjelmointirajapintojen hallinnan ja tiedonsiirron ratkaisuista keskusteltaessa ja linjattaessa.

Asiakirja on tarkoitettu pääasiassa arkkitehdeille, suunnittelijoille ja kehittäjille. Keskeisiä kohderyhmiä ovat:

* julkisen hallinnon toimijat, jotka tuottavat tietoa ja tarjoavat sitä edelleen omadatana
* julkisen hallinnon toimijat, jotka hyödyntävät toisten tarjoamaa omadataa
* yksityiset tahot, jotka hyödyntävät tai tuottavat julkisen hallinnon tarjoamaa omadataa
* tietojärjestelmäintegraattorit ja ohjelmistotalot.

## Rajaukset ja reunaehdot

* 1. Julkisen hallinnon omadata-arkkitehtuurissa käsitellään henkilötietojen käyttöä ja hallinnointia omadatana tilanteessa, jossa rekisterinpito kuuluu julkisen hallinnon organisaatioille, joiden tiedonkäsittelyoikeus perustuu voimassa olevaan lainsäädäntöön.
  2. Käsitellään vain luonnollisten henkilöiden tietojen käyttöä.
  3. Käsitellään suostumuspohjaista henkilötietojen käyttöä julkisen hallinnon keinona mahdollistaa lakisääteisten peruspalvelujen ulkopuolisia, lisäarvoa tuottavia tietointensiivisiä tai -pohjaisia palveluja.
  4. Omadata-näkökulma täydentää suostumuksen avulla lakisääteistä tiedon käsittelyä. Tiedon käsittelyn kieltäminen ja vastustaminen muussa kuin tiedon käytön alkuperäisessä käyttö- tarkoituksessa sisältyy käyttötapauksiin.
  5. Iteratiivisuus: Käyttökohteina, joiden perusteella arkkitehtuuri iteroidaan, pidetään 1. vaiheessa (1-2 vuotta) konkreettisia, suostumuksen avulla tiedon luovutusta suunnittelevia tahoja: varmimpana esillä on Koski-koulutustiedon palvelu (opiskelijastatuksen todistaminen 3. osapuolelle), alustavina visioina on listattu Omavero (verotustiedon luvittaminen yksityisen palvelun käyttöön), Trafin autojen vertaisvuokrauspalvelu ja Helsingin kaupungin Minun Helsinkini -palvelu. Nämä käyttötapaukset on kuvattu osin asiakirjan luvussa [Toiminnallinen omadata-arkkitehtuuri](#_qr8jn5pe7bsd) ja tarkemmin dokumentin liitteissä.
  6. Arkkitehtuurin 2. vaiheen (korkean arkkitehtuurillisen kypsyystason) tavoitetilaa käsittelevät osiot antavat suosituksia omadata-palveluihin ja sitä kautta laajemmin julkisen hallinnon palvelukehitykseen liittyvistä komponenteista, mutta eivät määritä varsinaisia toteutustapoja tai aikatauluja.

# 

## Asiakirjassa käytetty terminologia ja sanasto

**Henkilötietoa** on kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön (‘**rekisteröity**’) liittyvä tieto. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

**Rekisterinpitäjä** on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muuta elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

**Käsittely** tarkoittaa toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.

**Henkilötietojen käsittelijä** on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

**Kolmannella osapuolella** tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta toimielintä kuin rekisteröityä, rekisterinpitäjää, henkilötietojen käsittelijää ja henkilöä, joilla on oikeus käsitellä henkilötietoja suoraan rekisterinpitäjän tai henkilötietojen käsittelijän välittömän vastuun alaisena.

**Vastaanottaja** on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, jolle luovutetaan henkilötietoja, oli kyseessä kolmas osapuoli tai ei.

**Omadata** on henkilöä koskeva data (koneluettava tieto), jota kyseinen henkilö voi itse hallinnoida ja hyödyntää.[[3]](#footnote-2)

**Suostumus** on määritelty EU:n yleisessä Tietosuoja-asetuksessa ([TsA](http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&from=FI)) seuraavasti: Rekisteröidyn suostumuksella tarkoitetaan mitä tahansa vapaaehtoista, yksilöityä, tietoista ja yksiselitteistä tahdonilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn antamalla suostumusta ilmaisevan lausuman tai toteuttamalla selkeästi suostumusta ilmaisevan toimen.

**Suostumusehdotus** (engl. consent notice) on suostumusta antavalle käyttäjälle rakennettu (yleensä sähköinen) ehdotusnäkymä, joka kuvaa ja dokumentoi pyydetyn suostumuksen yksilöivät tiedot: mitä tietoja halutaan käsitellä, mistä palvelusta on kyse, mihin käyttötarkoitukseen tiedot menevät, siirtyvätkö tiedot pyytävältä osapuolelta eteenpäin kolmansille osapuolille. Ehdotuksessa tulee kuvata mitkä pyydetyt tiedot ovat ehdottoman tarpeellisia, mitkä valinnaisia. Ehdotuksen toteuttamiseksi helposti ymmärrettävällä tavalla voidaan hyödyntää esimerkiksi selventäviä ikoneja tai kuvia.

**Suostumustallenne** dokumentoi Tietosuoja-asetuksessa vaaditun todistettavissa olevan suostumuksen. Tallenne on yksikäsitteinen rekisteröidyn, luvitetun tiedon ja sen lähde- ja kohderekisterit/palvelut listaava, koneluettava, allekirjoitettu tallenne jolla on uniikki tunniste, luontipäivämäärä, viimeinen suostumuksen voimassaolopäivämäärä ja nykytila (aktiivinen, passiivinen tai revokoitu).

**Omadatapalvelu** on digitaalinen palvelu, joka joko tarjoaa tai pyytää käyttöönsä henkilötietoa, jonka käyttö on rekisteröidyn suostumuksen alaista.

**Valtuus** on toimivalta eli henkilön oikeus asioida toisen (luonnollisen henkilön tai oikeushenkilön) puolesta tietyssä asiassa. Valtuutuksella luodaan valtuus.

**Valtuutus** on tahdonilmaisu, joka on annettavissa luonnollisen henkilön toimesta joko toiselle luonnolliselle henkilölle tai oikeushenkilölle. Valtuuttaja valtuuttaa valtuutetun asioimaan puolestaan tietyssä asiassa. Valtuutuksella tarkoitetaan siis kansalaisen toiselle henkilölle antamaa valtuutusta, eli joku muu on saanut oikeuden toimia luonnollisen henkilön puolesta ikään kuin olisi henkilö itse[[4]](#footnote-3). Lopputuloksena syntyy valtuus.

**Suomi.fi-palveluhallinta** **(PaHa)[[5]](#footnote-4)** on organisaatioiden itsepalveluportaali Suomi.fi-palveluiden käyttöönottoa varten. Palveluiden käyttöönotto ja hallinta edellyttävät organisaatioilta tunnistautumista ja rekisteröitymistä Palveluhallintaan. Organisaatio hyväksyy portaalissa käyttämiensä palveluiden käyttöehdot sekä täyttää tarvittavat luvat ja hakemukset; teknisissä hallintanäkymissä organisaatio voi suorittaa itsepalveluna palveluihin liittyvää järjestelmien asetusten määrittämistä.

**Suomi.fi-palvelutietovaranto (PTV)[[6]](#footnote-5)** on keskitetty tietovaranto, johon organisaatiot, joilla on joko käyttövelvollisuus tai käyttöoikeus, tuottavat tiedot tarjoamistaan palveluista ja asiointikanavista sekä palveluun kytkeytyvän organisaation tiedoista. Tiedot ovat nykyisellään varannossa lähinnä ihmisluettavassa muodossa.

Tiedon **käsittelyperuste** on yksi TsA:n määrittämistä henkilötiedon käsittelyn juridisista perusteista: 1) sopimus, 2) suostumus, 3) rekisterinpitäjää koskeva lakisääteinen velvoite tai 4) julkinen etu, 5) rekisteröidyn terveyteen liittyvä elintärkeä etu tai 6) rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu. Julkishallinnon lakisääteisissä palveluissa ei ole mahdollista käyttää perusteena 1) tai 6) -käsittelyperustetta.

**Yhteentoimivuusvälineistö** on alusta, jonka tavoitteena on parantaa ja yhtenäistää tietosisältöjen määrittelyä luomalla yhteinen tapa hallita, tuottaa ja ylläpitää julkishallinnon palveluiden taustalla olevia tietomäärityksiä ja metatietoja. Yhteentoimivuusvälineistö koostuu sanastoista, koodistoista sekä tietomalleista sekä sanastojen julkaisuun tarkoitetusta palvelusta.

**Ohjelmointirajapinta (API, sovellusrajapinta)** on digitaalinen itsepalveluna tarjoiltu tietotuote, jota hyödynnetään ja myydään palveluna. Tietotuotteen käyttöönotto ei saa kestää 5 minuuttia kauempaa. Tuossa ajassa sovelluskehittäjän pitää pystyä käyttämään tietotuotetta täysimittaisesti omassa ohjelmistossaan. Tähän tilanteeseen päästään toteuttamalla itsepalvelu käyttöönottoa varten:

* Nopea rekisteröityminen ilman turhia manuaalisia hyväksyntöjä ja mielellään valmiita sovelluskehittäjien käytössä olevia tunnuksia hyväksikäyttäen (esim. Github).
* Nimeämällä tietotuotteet kuvaavasti.
* Tarjoamalla paketti, jossa on esimerkkikoodit valmiina 1) tunnistukseen ja 2) sitten yksinkertaiseen datan kutsumiseen.
* API-avainten hallinta on hoidettu automaattisesti esimerkiksi [API-hallintaratkaisun](https://medium.com/apinf/apinf-enables-distributed-api-gateways-with-plethora-of-protocols-66f6d3a34396) tasolla.
* Tarkempi ja ajantasainen dokumentaatio tarjotaan syvempää ominaisuuksiin tutustumista varten.

**Omadata-palvelukuvaus** sisältää 1) ihmisen ymmärtämässä muodossa vapaamuotoisen kuvauksen palvelun tarjoamista ominaisuuksista, palveluntarjoajasta, käsiteltävien henkilötietojen käyttötarkoituksesta ja arvolupauksesta jota se asiakkaalleen tuottaa ja 2) koneluettavassa muodossa palvelun käyttämät tiedot ja niitä tarjoavat tekniset ohjelmointirajapinnat (viimeiset vain jos kyseessä on tietoja tarjoava Lähdepalvelu).

**Suostumustenhallintapalvelu** on digitaalinen (mikro)palvelu joka tarjoaa omadata-palveluille ja rekisterinpitäjille yhteisen ohjelmointirajapinnan palvelukohtaisten suostumusten luomiseen, olemassaolon tarkistamiseen, päivittämiseen tai poistamiseen.

**Notifiointi** on kansalaiselle välitetty tiedoksianto tunnetusta (lokitetusta) henkilötietojen käsittelystä julkishallinnon palveluissa tai rekistereissä. Notifiointeja voidaan kerätä ja toimittaa erilliseen palvelunäkymään joka kerää yksilölle tietoa henkilötietojen käytöstä hallinnossa.

**Käyttäjä** on luonnollinen henkilö joka hallinnoi omia tietojaan eri palveluissa henkilöasiakkaan roolissa. Juridisesta näkökulmasta Käyttäjä on rekisteröity (engl. data subject).

**Lähdepalvelu** on suostumustenhallinnan avulla omadataa toissijaiseen käyttöön tarjoava palvelu, tai organisaation tietorekisteri jos sillä ei ole käyttäjälle omaa palvelukäyttöliittymää.

**Hyödyntäjäpalvelu** on käyttäjän suostumuksen perusteella oman rekisteröidyn palvelukuvauksensa mukaisesti tietoja käsittelevä palvelu tai organisaatio.

**Luottamusverkko** on määrätyllä toimialueella toimijaverkoston yhteistä toimintaa sitova joukko määrityksiä, sääntöjä ja sopimuksia (engl. ‘A trust framework is a legally enforceable set of specifications, rules, and agreements governing the operation of a specific multi-party system.’).

**Henkilötiedon ensisijainen käyttö** on tiedon käyttöä sen ensisijaista käyttötarkoitusta varten (kuten lakisääteinen rekisterien ylläpito).

**Henkilötiedon toissijainen käyttö** l. **uusiokäyttö** tarkoittaa tiedon käsittelyä erikseen osoitettuun käyttötarkoitukseen joka ei ole listattu alkuperäisen käytön kuvauksessa tai laissa.

**Suomi.fi-palveluväylä[[7]](#footnote-6)** on Suomessa käyttöönotettu, Viron X-Road-ratkaisuun perustuva standardi tapa siirtää tietoa tietovarantojen ja niitä hyödyntävien tietojärjestelmien välillä.

**Liityntäpalvelin** (engl. Security Server) on Suomi.fi-palveluväylän keskeinen komponentti, jonka kautta tietolähteiden ja tietojärjestelmien liittäminen palveluväylään tapahtuu. Jokaisella palveluväylään liitetyllä järjestelmällä on oltava käytössään liityntäpalvelin, jonka kautta kaikki palveluväylään lähetettävät tai sieltä vastaanotettavat sanomat kulkevat.

**X-Road** on Virossa kehitetty ja käytössä oleva ohjelmisto, joka toimii osana Suomi.fi-palveluväylän teknistä ydintä.

**SOAP** (engl. Simple Object Access Protocol) on XML-kieleen pohjautuva tietoliikenneprotokolla, jota Suomi.fi-Palveluväylän liityntäpalvelimen rajapintatoteutuksessa käytetään.

**NIIS** (engl. Nordic Institute for Interoperability Solutions) on [Suomen ja Viron yhteinen instituutti](https://www.niis.org/) joka vastaa Suomi.fi-palveluväylän ja X-road alustan yhteiskehityksestä 2018 alkaen.

**WSDL** (engl. Web Service Description Language) on - on W3C:n määrittämä XML-perustainen kieli, jolla kuvataan tietoverkossa tarjolla oleva web-teknologioihin perustuva sovelluspalvelu, eli Web Service. Ks. tarkemmin [WSDL](https://fi.wikipedia.org/wiki/WSDL).

**REST** (engl. **Re**presentational **S**tate **T**ransfer) on HTTP-protokollaan perustuva arkkitehtuurimalli ohjelmointirajapintojen toteuttamiseen. Syrjäyttämässä aiemmin yleisen WSDL/SOAP mallin. Ks. [kappale 5](http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm) Roy Fieldingin väitöskirjasta vuodelta 2000.

**JSON** (engl. Javascript Object Notation) on datan esitysmuotoilu, joka tarjoaa standardoidun tiedonvaihtomuodon käyttämällä yksinkertaisesti tekstiä. Tarkka englanninkielinen syntaksin määrittely löytyy [RFC4627](https://www.ietf.org/rfc/rfc4627.txt). Suomenkielinen esittely <http://wiki.freepascal.org/JSON/fi>.

# 

# Periaatetason arkkitehtuurikuvaukset

Omadata-arkkitehtuurin keskeiset periaatteet ja toimintaympäristön visio on kuvattu tässä kappaleessa.

Tätä asiakirjaa kirjoitettaessa on pyritty huomioimaan MyData muutosvoimana -raportissa esitetyt MyData -periaatteet:[[8]](#footnote-7)

*“****1. periaate: Ihmiskeskeinen tiedonhallinta ja yksityisyys***

*Ensimmäisen MyData-periaatteen mukaan yksilöt tulisi nähdä aktiivisina toimijoina, ei passiivisina toiminnan kohteina. Ihmisillä tulee olla paitsi oikeuksia suhteessa omaan tietoonsa, myös käytännön työkaluja tiedon hyödyntämisen ja yksityisyytensä hallintaan. Henkilön tulisi voida siirtää tai kopioida itseään koskeva tieto muiden käyttöön, ja myös lopettaa tällainen jakaminen helposti. Parhaimmillaan oman tiedon käyttöä voisi valvoa ja tehdä sitä koskevia yksityiskohtaisia valintoja. Ihmiskeskeinen tiedonhallinta merkitsee myös, että yksilöä koskeva tieto eri lähteistä olisi kokonaisvaltaisesti ja helposti saatavissa. Yksilö on tietoja yhdistävä tekijä riippumatta siitä, mihin tiedot on talletettu. Ottaessaan käyttöön uusia palveluita käyttäjä voi valita, mitä itseään koskevia tiedon lähteitä hyödyntäisi.*

***2. periaate: Käytettävä data***

*Toinen periaate ehdottaa, että rekistereihin ihmisistä kerätty tieto tulisi nähdä uudelleen käytettävänä resurssina. Tällä hetkellä palvelut, jotka keräävät tai käsittelevät tietoa ihmisistä, tallentavat ja soveltavat tietoja ennalta määriteltyihin käyttötarkoituksiin. Yksilöt sen sijaan voivat hyötyä näistä tietovarannoista käyttämällä niitä joustavasti itse määrittelemiinsä tarkoituksiin. Datan käytettävyys edellyttää, että tietoon on helppo päästä käsiksi ja että se on esitetty muodossa, joka mahdollistaa uudelleenkäytön.*

***3. periaate: Liiketoimintaympäristön avoimuus***

*Ihmiskeskeinen tiedon hyödyntäminen voi tukea avoimia liiketoimintamalleja, joissa asiakkuuden vaihto on helppoa ja tieto seuraa ihmisten mukana. Julkishallinto ei luonnollisesti toimi liiketoiminnallisin perustein. Sen piirissä yksittäiset toimijat ovat usein ainoita, jotka keräävät jotakin tietoa viranomaistehtäviään varten. Tästä huolimatta julkinen sektori voi pyrkiä luomaan avoimen toimintaympäristön MyDataan pohjaavien palveluiden kehittäjille, mikä voi tukea niin yksityisen sektorin sovelluksia kuin julkishallinnon sisäistäkin toimintaa. Yhteisiä ja avoimia standardeja käytettäessä toimijoita ei suljeta pois käyttämästä tietoresursseja. Silloin kun palveluita syntyy monipuolisesti, eivät käyttäjätkään ole riippuvaisia yksittäisistä palveluntarjoajista tai käyttöliittymistä.”*

## Omadatan käyttötarpeet julkishallinnossa, nykytilanne ja (liike)toimintaympäristö

Julkinen hallinto kerää paljon arvokasta tietoa kansalaisista, joka käyttö on usein tarkkaan lainsäädännössä rajattu. Suomessa on erilaisten selvitysten[[9]](#footnote-8) mukaan noin 800 erilaista lakia ja asetusta, jotka säätelevät henkilötietojen käyttöä. Osa näistä on hyvinkin yksityiskohtaisia; laissa määritellään sekä kerättävät tiedot että niiden käyttötarkoitus hyvinkin yksityiskohtaisesti. Kerättävien tietojen käsittelyyn kulutetaan huomattavasti resursseja, mutta niiden hyödyntämisessä olisi paljon nykytilaa enemmän mahdollisuuksia. Omadata on keino sopimusteknisesti laajentaa kansalaisen omalla suostumuksella näiden tietojen hyödyntämistä osana tietoyhteiskuntaa ja digitaalisia palveluita.

Omadatan käsitteellä tarkoitetaan henkilötietojen käytön hallinnan mahdollistamista rekisteröidylle itselleen. Omadata-lähestymistapa ja toteutukset eivät muuta viranomaisen asemaa ensisijaisena rekisterinpitäjänä ja tiedon kerääjänä - omadata painottaa yksilön oikeuksia nähdä omat tietonsa ja yksilön suostumukseen perustuvaa tiedon hallittua ja läpinäkyvää käyttöä muissa rekisterinpitäjän tai ns. kolmansien osapuolten tuottamissa palveluissa.

## Suostumus

Yleisesti viranomaisten toimesta tehtävästä henkilötietojen käsittelystä ja rekistereistä säädetään henkilötietolaissa, julkisuuslaissa sekä moninaisissa sektorikohtaisissa erityislaeissa. Nykyisen henkilötietolain 3 §:n mukaisesti suostumuksella tarkoitetaan *kaikenlaista vapaaehtoista, yksilöityä ja tietoista tahdon ilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn*.

Tietosuoja-asetuksen myötä yksilön tiedollinen itsemääräämisoikeus ja oikeus hallita omien henkilötietojensa käsittelyä suostumuksen avulla on korostunut. Suostumus ei kuitenkaan edelleenkään ole ensisijainen käsittelyperuste henkilötietojen käsittelylle viranomaistehtävässä.

Yksilöityjen suostumusten avulla voidaan mahdollistaa alunperin julkista palvelutehtävää tai muuta viranomaiskäyttöä varten kerätyn tiedon hyödyntäminen yksiölle lisäarvoa tuottavissa muissa digitaalisissa palveluissa. Yksilöä koskevat, luovutettavissa olevat tiedot eri rekistereistä voidaan kerätä hyödyntävän palvelun käyttöön automaattisesti kysymällä sähköinen suostumus (engl. consent) tietojen siirtoon ja tallentamalla tämä suostumus koneluettavassa muodossa suostumustenhallintapalveluun. Uudenlaisen infrastruktuurin avulla on mahdollista yksinkertaistaa tietopyyntöihin liittyviä nykyisiä hallinnon prosesseja ja sujuvoittaa tiedon liikkumista. Tämä luo mahdollisuuksia myös julkisen hallinnon roolin muutokseen.[[10]](#footnote-9)

Tietosuoja-asetuksen myötä on oletettavissa, että henkilötiedon käsittelyn läpinäkyvyyteen ja kansalaisen suostumukseen pohjautuvien digitaalisten, henkilötietoja käsittelevien palvelujen tarjonta kasvaa. Henkilötietoa hyödyntäviä palveluita tarjoavat erityisesti yksityisen sektorin toimijat, mikä voi luoda uudenlaista vuorovaikutusta sekä julkisen hallinnon ja yksityisten toimijoiden että kansalaisten välille. Suostumusperusteinen tiedon hyödyntäminen palveluissa voi synnyttää myös uudenlaista avoimuutta; esimerkiksi yksilöiden automaattiseen profilointiin hyödynnettävien algoritmien tulisi olla siinä määrin läpinäkyviä ja helppotajuisesti selitettyjä, että yksilö tietää, millä perusteella hän määräytyy profiiliinsa.

Henkilötiedon luovutuksen ja käytön luvittamisesta omadata-periaatteiden mukaisesti vastaavan toimijan rooli nähdään operaattorina. Suostumuksia ja niihin liittyviä palveluja hallinnoiva toimija on tarkoitettu toimimaan osana laajempaa operaattorien verkostoa, jossa operaattorit toimivat sidottujen sääntöjen ja yhteensopivan infrastruktuurin sisällä. Esimerkkinä vastaavasta on vahvan tunnistamisen luottamusverkosto pankkien, teleoperaattoreiden ja Väestörekisterikeskuksen välillä. Yksilön on mahdollista vaihtaa luottamusverkoston sisällä palvelua niin halutessaan. Tiedon käytön luvittamista tarjoavilla operaattoreilla on laaja pääsy ihmisten henkilötietoihin tai vähintään tietoon niiden käytöstä jossakin palvelussa. Tiedon hallinta omadatana laajentaa ja muuttaa yksilön luottamussuhdetta suostumusten hallintapalvelua tarjoavaan toimijaan kokonaisvaltaisempaan suuntaan. Julkisen hallinnon roolin omadatassa ei tarvitse rajoittua vain luotettavaksi tiedon lähteeksi: tiedon hallintaan liittyvät suostumukset ja niiden hallinta on nykyhetkessä rajoitettu liiketoimintamalli yksityisille yrityksille, mutta pohjoismaisessa toimintaympäristössä julkista hallintoa voidaan pitää luotettavana operaattoritoimijana. Palveluiden suunnittelua ja rakentamista tulee tarkastella vahvasti loppukäyttäjän eli usein kansalaisen (yleisemmin henkilöasiakkaan) näkökulmasta, jonka tiedollista itsemääräämisoikeutta toimilla on tarkoitus tehostaa. Luotavat arkkitehtuurikuvaukset ottavat kantaa operaattorimalliin.

## Käsittelystä notifiointi

Tietosuoja-asetus vaatii rekisterinpitäjiltä myös läpinäkyvyyttä henkilötietojen käsittelystä. Osin tätä vastuuta voidaan kantaa kuvaamalla rekisterin tai palvelun tietosuojaselosteessa selkeämmin mihin tarkoituksiin ja kenen (organisaation, kolmannen osapuolen tai henkilöiden) toimesta tietoja käsittelyn yhteydessä käytetään, vaikka tiedon käsittely ei olisi puhtaasti yksilön hallinnassa. Tällaista läpinäkyvyyttä tulee vision mukaan tukea myös kehittämällä rekisterinpitäjien lokimekanismeja kuluttajaviestinnän suuntaiseksi: rekisteröidyn tietojen käsittelystä eri organisaatioissa tulisi kansalaisen niin halutessaan saada tietoa esimerkiksi (push-) viestinä tai kirjauksena tietosuojalokiinsa, joka olisi loogisesti suostumuksienhallintapalvelulle rinnakkainen toiminta, esimerkiksi Suomi.fi:ssä. Rekisterinpitäjät on jo velvoitettu keräämään teknisiä lokitietoja aukottoman kirjausketjun osoittamiseksi, käytännössä kyse on visiossa näiden lokien muotoilusta luottamusta ja läpinäkyvyyttä lisääviksi uusiksi palveluiksi.

## Kiellot ja käsittelyn vastustaminen

Henkilötietojen käsittelyn uuteen EU-laajuiseen lainsäädäntöön kuuluu myös yksilön oikeus vastustaa tai kieltää henkilötietojen käsittely tiettyjen Tietosuoja-asetuksen määrittelemien käsittelyperusteiden alla toimivissa palveluissa. Käsittelyn vastustamisen mahdollisuus tulisi huomioida ao. palveluissa, rekisteröidä se osaksi palvelun ihmis- ja koneluettavaa palvelukuvausta ja asetuksen ohjeistuksen mukaisesti tarjota käyttäjälle käsittelyn kielto- tai vastustamistoiminteet asianmukaisessa näkymässä. Myös kiellot ja vastustamispyynnöt voisi kehittää omaksi yhteiseksi palvelukseen. Nykytilassa käsittelykieltoja on olemassa ainakin Kelan Kanta-palvelujen yhteydessä.

## Suostumusten siirrettävyys

Tiedon luovutukseen ja käyttöön annettujen suostumusten siirrettävyys voidaan nähdä analogisena tapauksena puhelinnumeron siirrettävyydelle operaattorilta toiselle, tai eri palveluntarjoajien pankkitunnistautumisen käytölle vahvassa tunnistautumisessa. Suostumusten siirrettävyys voi kuitenkin rajoittua yksityisen sektorin palveluiden välillä tehtyihin suostumuksiin: julkinen sektori ei mitä todennäköisimmin voi ulkoistaa kansalaisten tietojen käytön suostumustenhallintaa muille kuin itse erikseen hyväksymilleen tahoille.

Lähtökohtaisesti suunnittelussa noudatetaan periaatetta jossa kansalaisen omadataan (luovutettavissa olevaan henkilötietoon) liittyvät suostumukset, notifioinnit, käsittelykiellot ja muut palveluasetukset (niin kutsuttu ‘omadata-tili’ sisältöineen) Suomi.fi -palveluissa ovat itsessään kansalaisen hallinnoitavissa olevaa omadataa.

## Nykytila kansallisen palveluarkkitehtuurin ja tiedon hallinnan näkökulmasta

Omadata, henkilötiedon hyödyntäminen suostumuspohjaisesti, on monitahoinen ilmiö ja vaatii tarkastelua niin lainsäädännön, toiminnan, tiedon, tietojärjestelmien kuin teknologian näkökulmista.

Digitalisoinnin periaatteet[[11]](#footnote-10) linjaavat tiedon hallinnan käytänteitä; uutta (samaa) tietoa tulisi pyytää vain kerran ja rajapinnat tulisi avata yrityksille ja kansalaisille. Periaatteiden toteuttaminen ja toteutuminen vaatii selkeän kokonaiskuvan julkisen hallinnon hallussa olevasta tiedosta. Mikäli tietoja halutaan kysyä ainoastaan kerran tai edelleen hyödyntää suostumukseen perustuen, pitää tiedon semanttinen yhteentoimivuus ratkaista, jotta varmistetaan, että siirtyvä tieto, esimerkiksi “palkka”, ymmärretään samalla tavalla niin lähettäjän kuin vastaanottajan puolella ja myös tietoa luvittavan taholla. Julkisen hallinnon toimijoiden tulee siis kuvata hallinnoimansa tietovarannot ja niiden tiedot metatietojen tasolla yhtenäisesti. Tämä lähestymistapa mahdollistaa tulevaisuudessa laajasti tiedon hyödyntämisen - myös sellaisen tiedon, jolla ei ehkä juuri tällä hetkellä nähdä arvoa, mutta jonka rooli voi myöhemmin muuttua. Tietovarantojen kuvaaminen koneluettavuuden mahdollistaen vaatii tukipalveluita, kuten “Kansallisen metatietovarannon” avoimen tiedon palvelun (avoindata.fi) rinnalle sekä koordinoidusti hallinnoidut, tiedon semanttisen yhteentoimivuuden mahdollistavat metatietoresurssit, muun muassa sanastot ja luokitukset, ja niiden hallinta- ja jakeluratkaisut. Koneluettavuuteen nojaavat tiedon hyödyntämisen tietovirrat ja toisaalta laajeneva joukko tiedon hyödyntäjiä synnyttävät vaatimuksen tiedon semanttiselle yhteentoimivuudelle myös julkisen hallinon ulkopuolella, muun muassa tietoa hyödyntävillä yksityisillä tahoilla.

Tiedon integraatiota tulee tarkastella tiedon semanttisen yhteentoimivuuden ja siirron näkökulmista. Tiedon siirron mahdollistamiseen toteutetun kansallisen ratkaisun, Suomi.fi-palveluväylän (engl. X-Road) ohjelmistoarkkitehtuuri on pitkälti sen alkuperäiseltä suunnitteluvuodelta (2001) peräisin. Sen WSDL/SOAP -ratkaisut toimivat tiettyyn rajaan asti kokonaisvaltaisen tiedonhallinnan kanssa. Omadatan mahdollistaminen on teknisestä näkökulmasta käytännössä ohjelmointirajapintojen hallintaa. Ohjelmointirajapintojen avulla toteutettavat tietovirrat vaativat älykkäät analytiikka- ja tietoturvapalvelut, joiden avulla niiden palvelutasot voidaan paremmin hallita. Kehitystarvetta Palveluväylän ja siihen liittyvän liityntäkatalogin ohjelmistoarkkitehtuuriin syntyy, koska rajapintateknologiat kehittyvät nopeasti. Tämän hetken de facto standardi ohjelmistorajapinnoissa on REST/JSON, jonka kehitystarve onkin jo nostettu esille Palveluväylän kehityksessä ja sitä tulee viemään eteenpäin Palveluväylän kehityksestä vastaava taho the Nordic Institute for Interoperability Solutions (NIIS).

Suomi.fi-valtuudet mahdollistaa henkilön puolesta-asioinnin. Palvelussa käytetään geneerisiä valtuutuskoodeja. Henkilötietojen suostumusperusteinen lähestymistapa menee huomattavasti tätä yksityiskohtaisemmaksi tietojen luvittamisen kanssa; jopa yksittäisiä tietoja (esimerkiksi etunimi, sukunimi, sähköpostiosoite) luvitetaan eri palveluiden kesken.

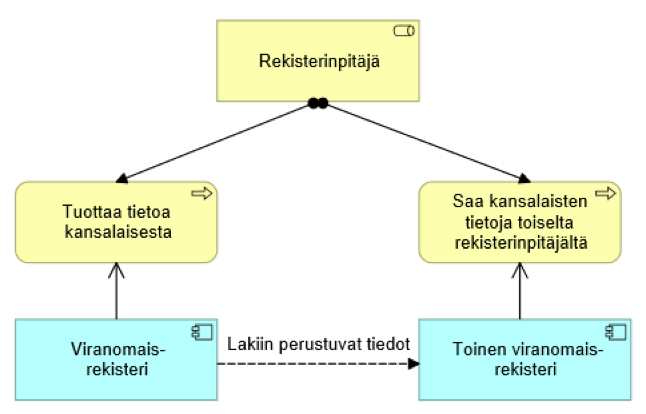
Suomi.fi-palvelutietovarantoon (PTV) julkishallinnon organisaatioilla on ns. KaPA-lain (laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista 571/2016) myötä velvollisuus kuvata palvelunsa PTV:n. Myös yksityiset toimijat voivat kuvailla palveluita sinne. Sen nykyinen tietomalli ei sisällä tietoja palveluiden digitaalisista palvelumalleista, kuten ohjelmointirajapinnoista, koska sen käyttötarkoitus on kansalaisten informoiminen julkishallinnon palveluista. Internetin päätelaitteiden erilaisuuden kasvaessa (erilaisista älypuhelimista suuriin taulutelevisioihin ja jokapaikan tietotekniikkaan) ei graafinen nettisivu ole enää tärkein käyttöliittymä tietoon. Näin ollen “yhden luukun periaate” ei enää edusta yhtä nettisivua, vaan enemmänkin ohjelmointirajapintojen keskitettyä haku- ja katalogipalvelua. Tietoverkkoon kytkettyjen laitteiden määrä kasvaa jatkuvasti. Näin ollen Suomi.fi-verkkopalvelun sijaan tulisi tarkastella vaihtoehtoisesti ohjelmointirajapintalähtöistä tapaa tarjota julkisten tietovarantojen tietoja ja toimintoja. Ohjelmointirajapinnat voivat olla joko toiminnallisia rajapintoja, jolloin ne tarjoavat jonkinlaista tiedonkäsittelyä tai tiedon jakamiseen keskittyviä ohjelmointirajapintoja. Julkisen hallinnon tiedonkäsittely muodostuu jatkossa näiden verkostosta.

Suomi.fi-tunnistus palvelu tarjoaa vahvaa sähköistä tunnistautumista, joka tarkoittaa pankkien, mobiilioperaattoreiden tai VRK:n tarjoamia tunnistusratkaisuja. Henkilötietoihin liittyvät tunnistustarpeet vaihtelevat. Esimerkiksi monissa internet-palveluissa käytetään ns. “heikkoa tunnistamista” käyttäjän tunnistamiseen (Google, Facebook, Github ja suuri määrä salasanalla ja käyttäjätunnuksella toimivia palveluita). Toimivan henkilötiedon hyödyntämisen kannalta tunnistukseen tulisi tarjota kustannustehokas tapa hoitaa käyttäjän tunnistaminen nykyistä erilaisemmin tavoin. Lisäksi huomiota tulee kiinnittää käyttömäärien kasvuun, joiden ennustetaan kasvavan omadata-palvelujen myötä.

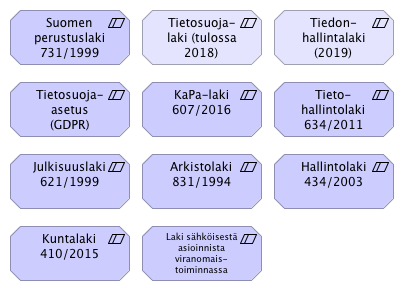
Suomi.fi -tuoteperhe on monin tavoin onnistunut palvelukokonaisuus. Sen toteutus oli julkisessa hallinnossa ensimmäinen laajan mittakaavan hanke, jossa toimintatapana hyödynnettiin ketterää ohjelmistokehittämistä ja avoimen lähdekoodin lähestymistapaa. Omadataan liittyvät ilmiöt vaativat samanlaista ennakkoluulotonta lähestymistä, sillä niiden monimutkaisuuden vuoksi usein ainoastaan hallitut kokeilut antavat kestäviä tuloksia. Usein tätä lähestymistapaa kuvataan Cynefin-viitekehityksellä. Cynefin jäsentää tavan johtaa työtä neljässä erilaisessa toimintaympäristössä: Yksinkertainen, vaikea, monimutkainen ja kaaoottinen.

## Lainsäädännöllistä selvitystä vaativat asiat

Asiakirja on laadittu tilanteessa, jossa säädöspohjan kehittäminen henkilötietojen käytölle omadata-periaatteiden mukaisesti on siirtymävaiheessa; toisaalta sovitetaan yhteen EU:n tietosuoja-asetusta ja kansallista lainsäädäntöä, uudistetaan tiedon hallinnan säädöspohjaa, mutta säädetään jo myös omadatatyyppiseen tiedon luovutukseen erityislakeja.



Kuva 2. Rekisteritietojen siirto perustuu nykytilassa aina sektorikohtaisiin erityislakeihin - tämä ei tule oleellisesti muuttumaan suostumuspohjaisen tiedonsiirron käyttöön ottamisen yhteydessä.



Kuva 3. Keskeiset julkishallinnon omadata-palvelujen kehittämiseen liittyvät yleislait

Uusien yleislakien säätämisen lisäksi on mahdollisesti tarpeen myös tehdä muutoksia jo olemassa oleviin säädöksiin. Alla olevassa taulukossa on pyritty asemoimaan omadata-konseptia nykyiseen lainsäädäntöön tarkemmin. Taulukossa listattujen säädösten lisäksi on olemassa lukuisia ns. sektorikohtaisia säädöksiä, joissa säädetään tiedonluovutuksesta. Tällaisia ovat esimerkiksi laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (SOTE-toimialue) tai laki liikenteen palveluista (liikenteen ja viestinnän toimialue). Sektorikohtaisia säädöksiä ei listattu tätä dokumenttia työstettäessä.

Alla oleva taulukko on alustava luonnos omadata-konseptin suhteesta horisontaalisiin säädöksiin (yleislakeihin) ja sitä tarkennetaan jatkovalmistelussa.

*Taulu 1. Omadata vs. olemassa olevat säädökset (LUONNOS)*

|  |  |  |
| --- | --- | --- |
| **Säädös** | **Pykälä / artikla** | **Huomioitavaa** |
| EU:n tietosuoja-asetus (GDPR, TsA) | 6 (1) a | Omadata –tyyppinen henkilötietojen käsittely on tämän mukaan lainmukaista, jos rekisteröity (henkilö) itse on antanut luvan tietojen käsittelyyn. EU:n tietosuoja-asetusta täydentämään saatetaan jatkossa säätää myös uusi kansallinen tietosuojalaki, joka on luonnollisesti huomioitava tavoitetilan malleja ja ratkaisuja tehtäessä.   * 6 artikla *”****Käsittelyn lainmukaisuus****; Käsittely on lainmukaista ainoastaan jos ja vain siltä osin kuin vähintään yksi seuraavista edellytyksistä täyttyy: a) rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten;”* |
| Henkilötietolaki | 3 §  8 §  12 §  13 §  23 § | Uusi tiedonhallintalaki tulee mahdollisesti kumoamaan Henkilötietolain ja pykälät siirtyvät uuteen lakiin (**tarkentuu jatkovalmistelussa).**    •3 § sisältää määritelmät mm. seuraaville: ’henkilötieto’, ’henkilötiedon käsittely’, ’suostumus’  •8 § *” Henkilötietoja saa käsitellä ainoastaan: 1) rekisteröidyn yksiselitteisesti antamalla suostumuksella;”*  •12 § *”Poikkeukset arkaluonteisten tietojen käsittelykiellosta; Mitä 11 §:ssä säädetään, ei estä: 1) tietojen käsittelyä, johon rekisteröity on antanut nimenomaisen suostumuksensa;”*  (**Tarkennettava jatkovalmistelussa**: myös arkaluonteista henkilötietoa voidaan siirtää omadatana?)  •13 § *”Henkilötunnuksen käsittely; Henkilötunnusta saa käsitellä rekisteröidyn yksiselitteisesti antamalla suostumuksella tai, jos käsittelystä säädetään laissa.”*  *23 § ” Poikkeusperusteet; Silloin kun siirto ei ole mahdollinen 22 tai 22 a §:n nojalla, voidaan henkilötietoja kuitenkin siirtää, jos: (24.11.2000/986) 1) rekisteröity on antanut yksiselitteisen suostumuksensa siirtoon”.*  Henkilötietoja voidaan siirtää henkilön suostumuksella EU:n ulkopuolellekin. |
| Hallintolaki | - | Hallintolaissa säädetään julkisen vallan käytöstä. Omadata –konseptiin ei liity julkisen vallan käyttöä (päätöksentekoa), joten Hallintolailla ei ole erityistä yhteyttä omadata -konseptiin **(tarkentuu jatkovalmistelussa**). |
| Tietohallintolaki | 7 § | Tietohallintolain kuvausvelvoitteen kautta sillä on välillinen yhteys omadataan: kuvausvelvoitteeseen sisältyy tietovarantojen kuvaaminen (tietysti sisältäen henkilötietojen kuvaukset).  •7 § ”*Julkisen hallinnon viranomaisen on julkisen hallinnon tietojärjestelmien yhteentoimivuuden mahdollistamiseksi ja varmistamiseksi suunniteltava ja kuvattava kokonaisarkkitehtuurinsa sekä noudatettava laadittua ja ylläpidettyä kokonaisarkkitehtuuria ja sen edellyttämiä yhteentoimivuuden kuvauksia ja määrityksiä sekä toimialakohtaisia tietojärjestelmien yhteentoimivuuden kuvauksia ja määrityksiä.”* |
| Julkisuuslaki | 16.3 §  26 §  29 § | Julkisuuslaki mahdollistaa henkilötietojen sekä henkilöön liittyvien muutoin salassa pidettävien tietojen luovuttamisen, mikäli siihen on saatu rekisteröidyn suostumus.  •16 § *”****Asiakirjan antamistavat****; Viranomaisen henkilörekisteristä saa antaa henkilötietoja sisältävän kopion tai tulosteen tai sen tiedot sähköisessä muodossa, jollei laissa ole toisin erikseen säädetty, jos luovutuksensaajalla on henkilötietojen suojaa koskevien säännösten mukaan oikeus tallettaa ja käyttää sellaisia henkilötietoja. Henkilötietoja saa kuitenkin luovuttaa suoramarkkinointia ja mielipide- tai markkinatutkimusta varten vain, jos niin erikseen säädetään tai jos rekisteröity on antanut siihen suostumuksensa.”*  •26 § *”****Yleiset perusteet salassa pidettävän tiedon antamiseen****; Viranomainen voi antaa salassa pidettävästä viranomaisen asiakirjasta tiedon, jos: 1) tiedon antamisesta tai oikeudesta tiedon saamiseen on laissa erikseen nimenomaisesti säädetty; tai 2) se, jonka etujen suojaamiseksi salassapitovelvollisuus on säädetty, antaa siihen suostumuksensa.”*  •*29 § ”****Salassa pidettävien tietojen antaminen toiselle viranomaiselle****; Viranomainen voi antaa toiselle viranomaiselle tiedon salassa pidettävästä asiakirjasta, jos: 1) tiedon antamisesta tai oikeudesta tiedon saamiseen on laissa erikseen nimenomaisesti säädetty; 2) se, jonka etujen suojaamiseksi salassapitovelvollisuus on säädetty, antaa siihen suostumuksensa;”* |
| Arkistolaki |  | (Tarkentuu jatkovalmistelussa) |
| Suomen peruslaki |  | (Tarkentuu jatkovalmistelussa) |
| Kuntalaki |  | (Tarkentuu jatkovalmistelussa) |
| Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista (Kapa-laki) | 8 § | Yksityiset elinkeinonharjoittajat voivat hyödyntää vain tiettyjä sähköisen asioinnin tukipalveluita (Suomi.fi –palveluita). Ne eivät voi esimerkiksi hyödyntää luonnollisen henkilön tunnistamiseen liittyvää tunnistuspalvelua. Omadata –konsepti kuitenkin edellyttää henkilön vahvaa tunnistamista. Voivatko yksityiset toimijat käyttää muuta yleisesti tarjolla olevaa tunnistuspalvelua jonka lähderekistereitä hallinnoivat viranomaiset voivat hyväksyä vahvaksi tunnistamiseksi?  8 § *”****Yksityisten käyttöoikeus ja käytön kieltäminen****;*  *Yksityiset yhteisöt, säätiöt ja elinkeinonharjoittajat saavat käyttää kansallista palveluväylää tietojen siirtoon.*  *Yksityiset yhteisöt, säätiöt ja elinkeinonharjoittajat saavat tarjotessaan palvelujaan yleisölle käyttää:*  *1) palvelutietovarantoa palvelujaan koskevien tietojen tarjoamiseen; 2) palvelunäkymiä ja asiointivaltuuspalvelua, jos niillä on oikeus käsitellä asiakkaidensa henkilötunnusta tai muuta tietojen pyytämisessä tai näyttämisessä tarvittavaa yksilöivää tunnusta palvelujensa tarjoamisessa.*  *Valtiovarainministeriön asetuksella voidaan säätää yksityisten yhteisöjen ja elinkeinonharjoittajien oikeudesta käyttää 3 §:n 2 momentissa tarkoitettuja tukipalveluja.” [palvelutietovaranto]* |
| Laki sähköisestä asioinnista viranomaistoiminnassa |  | (Tarkentuu jatkovalmistelussa) |

## 

# Toiminnallinen omadata-arkkitehtuuri

Toiminnallinen arkkitehtuuri on käyttötapauksissa kuvattu pääsääntöisesti vain tietystä näkökulmasta eli sellaisesta toiminnasta, jossa julkishallinnon rekisterinpitäjä luovuttaa lakisääteisen rekisterin tietoja henkilön suostumuksella yksityisen toimijan palvelun käytettäväksi. Kokonaiskäsityksen ja -ymmärryksen laajentamisen kannalta olisi suositeltavaa kuvata jatkossa myös muita mahdollisia näkökulmia, esimerkiksi omadatan siirtoa yhdeltä yksityiseltä toimijalta toiselle yksityiselle toimijalle. Tieto voi siirtyä erilaisilta toimijoilta toisille ja kumpaankin suuntaan. Mahdollisia variaatioita on hahmoteltu alla olevaan taulukkoon.

*Taulu 2. Mahdollinen omadata-perusteinen tiedonvaihto eri osapuolten välillä tavoitetilassa.*

|  |  |  |
| --- | --- | --- |
| **Tietoa tuottava** | **Tietoa hyödyntävä** | **Kuvaus** |
| Julkisen sektorin organisaatio | Henkilö itse | Henkilö voi halutessaan kerätä omat tietonsa eri rekisterinpitäjiltä omadata-tietopankkiin (ns. MyData -tili, jossa on mukana oma tietovaranto). |
| Henkilö itse | Julkisen sektorin organisaatio | Omadatan hyödyntäminen esimerkiksi hakemuksia jätettäessä. |
| Julkisen sektorin organisaatio | Yksityinen palveluntarjoaja (henkilö itse) | Henkilön suostumuksella tietoa voidaan siirtää yksityiselle palveluntarjoajalle, tällöin tietoa hyödyntävät sekä henkilö itse että yksityinen palveluntarjoaja. |
| Yksityinen palveluntarjoaja | Henkilö itse | Henkilö voi halutessaan kerätä omat tietonsa eri rekisterinpitäjiltä omadata -tietopankkiin (ns. MyData -tili tietovarannolla). |
| Yksityinen palveluntarjoaja | Julkisen sektorin organisaatio (henkilö itse) | Joissain tapauksissa voisi olla mahdollista ja järkevää siirtää tietoa myös näin; tässäkin tapauksessa tiedonvaihdosta lisäarvo syntyy ensisijaisesti henkilölle. |

.

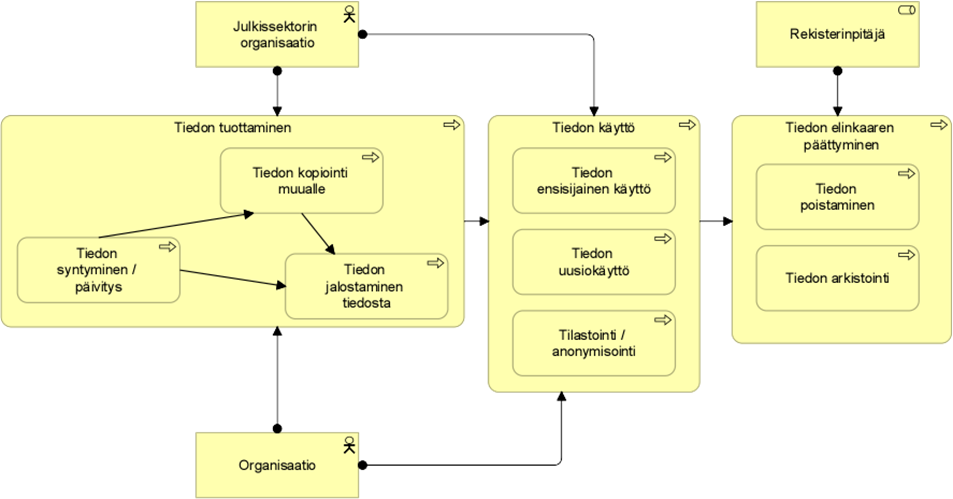
Käyttötapausten kuvausten yhteydessä listattiin ylös sekä havaintoja että vaatimuksia omadatan tavoitetilan arkkitehtuurille. Keskeisimmät vaatimukset on pyritty huomioimaan tavoitetilaa suunniteltaessa.

**Toiminta-arkkitehtuurin kuvauksessa esiin nousseet keskeiset havainnot ja vaatimukset:**

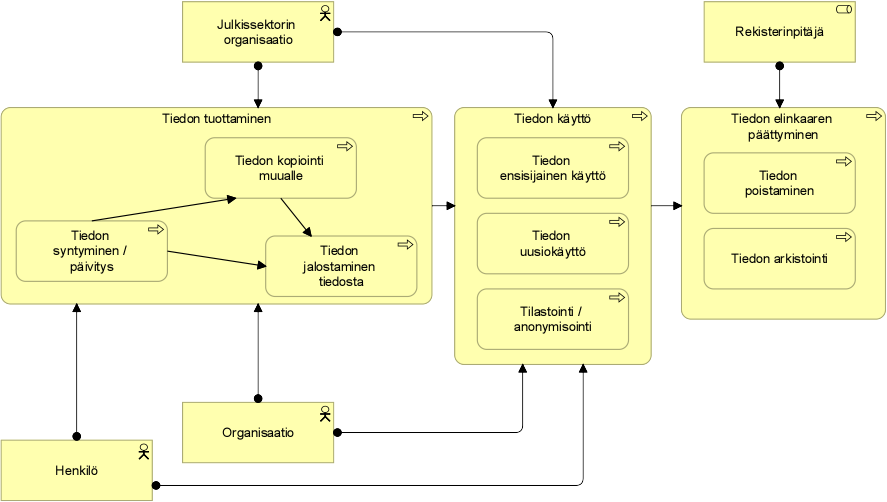
* Henkilöiden tietojen siirtoon rekisteristä toiseen on nykytilassa käytössä erilaisia tapoja. Esimerkiksi:
  + Lakiin perustuvat tietojen massasiirrot; jotka eivät ole omadataa, sillä näihin ei tarvita suostumuksia ja suuren tapahtumamäärän takia nämä kannattaa jatkossakin tehdä mm. eräajoina (verotukseen liittyvien tietojen kerääminen eri lähteistä verottajalle, oppilaitoksiin hyväksymisten ilmoittaminen Kelaan).
  + Pyynnöstä tapahtuvia luovutuksia, kun organisaatio pyytää tietyn henkilön tietoja toiselta organisaatiolta); johon voidaan tarvita henkilön suostumus tai ei (erityisesti terveydenhuollossa käytetään tätä).
* Tietojen luovutusta (suostumuksia ja kieltoja) säädellään erityislaeissa ja toimintatavat ovat erilaisia eri hallinnonaloilla.
* Verkostomaisen toimintatavan mahdollistamiseksi kannattaa selvittää sitä varten kehitettyjen uusien teknisten ratkaisujen tarjoamia mahdollisuuksia, kuten lohkoketjuteknologiat (esimerkiksi Sovrin).
* Käyttäjän asiointipolku vaihtelee; pääsääntöisesti omadatan siirtoon liittyvä suostumus todennäköisesti kuitenkin annetaan siinä palvelussa, johon tietoja halutaan siirtää (julkissektorin rekisteristä).
* Omadata -tiedonsiirtokonseptilla ei voi eikä kannata korvata nykyistä viranomaisten välistä, lakisääteistä tiedonvaihtoa.
* Eri sidosryhmien (=toimijoiden) rooleja pitää tarkentaa; missä roolissa mikäkin organisaatio voi toimia? Erityisen ongelmallisia ovat ”hybridiorganisaatiot”, jotka osittain vastaavat julkishallinnon tehtävistä ja osittain ovat yksityisiä toimijoita.
* Erilaiset tunnistautumisvaatimukset tulevat asettamaan haasteita käytännön toteutuksille
  + Erityisesti paikallishallinnolle (kaupungit, kunnat) voi tulla tilanteita, joissa osa omadatan liitettävistä palveluista edellyttää vahvaa tunnistautumista ja osa ei; tuleeko tämä johtamaan siihen että on erilaista omadataa ja erilaisia suostumuksia? Esimerkiksi vain tietyn tyyppiseen omadataan liitetyt suostumukset pitää antaa vahvasti tunnistautuneena, osaan riittää ”kevyempi” rekisteröityminen?
* Kokonaiskäsityksen saamiseksi kuvaamistyötä kannattaisi vielä jatkaa eri näkökulmista;
  + Erilaisten toimijoiden välinen tiedonsiirto ja -vaihto (katso taulu 2)
  + Tiedonsiirtotavat ja eri variaatioiden asettamat vaatimukset ratkaisuarkkitehtuurille ja toteutukselle (esimerkiksi kertaluonteinen tiedonsiirto, määräajoin toistuva, muutostietopalvelun tarve).
* Yksityisiä toimijoita (rekisterinpitäjiä) koskevat eri vaatimukset kuin julkissektorin rekisterinpitäjiä; erityisesti yleinen tietosuoja-asetus määrittelee rekisteröidyille (henkilöasiakkaille) erilaisia oikeuksia suhteessa eri tahojen rekistereihin. Näiden erojen kuvaaminen kattavasti jatkotyössä voisi olla hyödyllistä, jotta varmistetaan että tulevat ratkaisut vastaavat eri tahojen vaatimuksiin.
* Julkissektorin rekisterinpitäjien tietopääoma eli rekisterien tietosisältö olisi syytä kuvata kattavasti. Kuvauksissa pitäisi huomioida erilaiset tiedon luokitteluun liittyvät näkökulmat ja vaatimukset, jotta kuvaustyöstä saataisiin optimaalinen hyöty.

Kuvatuista käyttötapauksista koottiin omadata-toimintaan liittyviä rooleja ja sidosryhmiä. Erityisesti rooleista hahmottui tiettyjä kokonaisuuksia. Tähän mennessä tunnistetut roolit voidaankin karkeasti ottaen jakaa kahteen ryhmään: 1) henkilön (yksilön) roolit sekä 2) digitaalisen liiketoiminnan roolit.

Nykytilassa tiedon tuottaminen ja hyödyntäminen on yksinomaan organisaatioiden hallinnassa. Omadata tulee merkittävästi muuttamaan tätä tilannetta, sillä tavoitetilassa myös henkilöllä voi olla rooli sekä tiedon tuottajana että hyödyntäjänä.

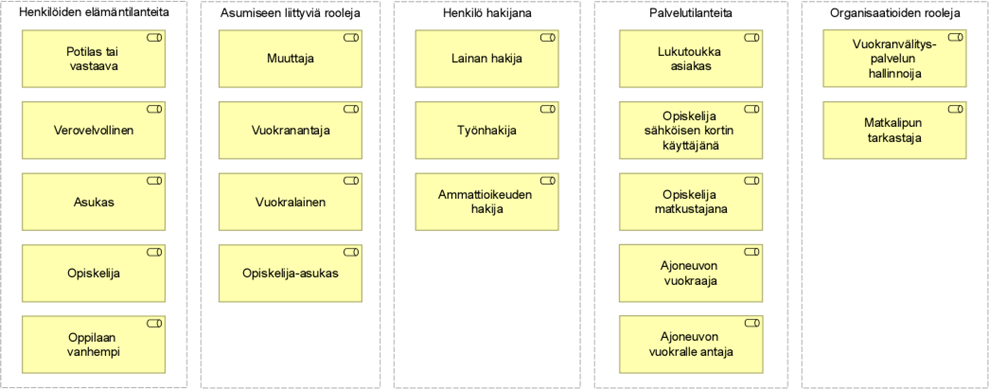


Kuva 4. Nykytilassa organisaatiot tuottavat tiedot, ovat rekisterinpitäjiä ja hyödyntävät tietoa.

Kuva 5. Tavoitetila: henkilöasiakkaan rooli sekä tiedon tuottajana että hyödyntäjänä.

Henkilöasiakkaalla on omadatan suhteen tavoitetilassa siis tietyllä tavalla dualistinen rooli. Toisaalta hän toimii omadatan “oheistuottajana” erilaisissa elämän tilanteissaan (tuottaa esimerkiksi omalla toiminnallaan tietoa opinnoista); toisaalta hän toimii tiedon hyödyntäjänä kun käyttää jotakin palvelua - esimerkiksi todistaessaan opiskelijastatuksensa ostaessaan matkalippua.

Henkilöllä voi samanaikaisesti olla omadataa monessa eri rekisterissä, sillä elämäntilanteet limittyvät toisiinsa.



Kuva 6. Roolit ja elämäntilanteet limittyvät toisiinsa, henkilö voi olla samaan aikaan useassa eri roolissa.

Digitaalisella liiketoiminnalla tarkoitetaan tässä sellaista liiketoimintaa, joka hyödyntää dataa digitaalisilla alustoilla ja käyttää automatisoituja M2M-yhteyksiä datan siirtoon. Tähän liittyvää liiketoimintamallia tai ansaintalogiikkaa ei käyttötapauksissa ole vielä juurikaan pohdittu. Tulevaisuudessa liiketoimintamallit varmaankin tulevat vaihtelemaan mm. sen mukaan millaisesta liiketoimintasektorista on kyse, mitä teknologiaa käytetään ja millaista maksua omadataa luovuttava taho tulee perimään. Kuvauksissa ei ole mukana juurikaan “puhdasta omadata -liiketoimintaa” eli niin sanotun MyData -operaattorin toimintaa. Jotakin sen tyyppistä on hieman mukana Lukutoukka-palvelun käyttötapauksessa, jossa henkilö voi yhdistellä tietoja eri lähteistä.



Kuva 7. Digitaaliseen liiketoimintaan liittyvät roolit

## Vaiheessa 1 identifioidut omadata-käyttötapaukset

Toiminnallisen arkkitehtuurin konkretisoimiseksi ja kokonaisuuden hahmottamiseksi kuvattiin neljän eri julkishallinnon organisaation kanssa kuvitteellisia tapauksia, joissa henkilö voisi hyödyntää yksityisten toimijoiden palveluissa tietojaan omadatana. Alle on nostettu näistä tapauksista neljä julkishallinnon ja yksityisen sektorin kesken verkotettua, käyttäjän suostumuksen käyttöön pohjautuvaa omadata-käyttötapausta. Opetussektorin käyttötapausta lukuunottamatta käyttötapaukset ovat kuvitteellisia.

1) Opiskelija-tiedon hyödyntäminen käytettäessä opiskelijaetuuksia

2) Verohallinnon Verotustietojen hyödyntäminen lainahakemuksessa

3) Helsingin kaupungin ‘Lukutoukka’ -palvelu

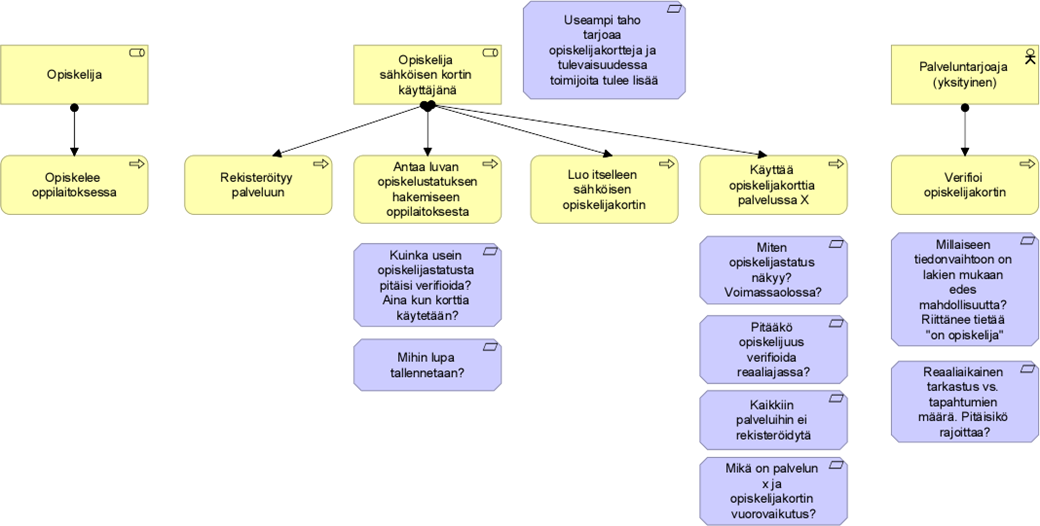
4) Trafin Ajoneuvon vertaisvuokraus -palveluiden mahdollistaminen.

Lisää kuvauksia löytyy liitteestä 1.

### Koulutus- ja opiskelutietojen hyödyntäminen

Opetustoimialalla tunnistettiin 11 käyttötapausta, joissa voitaisiin potentiaalisesti hyödyntää omadata -konseptin tyyppistä tiedonvaihtoa. Kaikki nämä potentiaaliset käyttötilanteet on kuvattu tarkemmin liitteessä 1.

Koska yksityiset toimijat ovat olleet erityisen kiinnostuneita opiskelijan läsnäolotiedosta, valittiin se esimerkiksi.



Kuva 8. Opiskelijan läsnäolotiedon hyödyntäminen opiskelijaetuuden käyttämiseksi   
yksityisen toimijan palvelussa

**Käyttötapausten kuvaamisen yhteydessä esiin nousseita vaatimuksia ja havaintoja:**

* Kuinka usein opiskelijastatusta pitäisi tarkistaa milloinkin? Kertaluonteisesti, määräajoin vai aina kun etuutta hyödynnetään? Erilaiset käyttötarpeet on huomioitava ratkaisua suunniteltaessa.
* Omadataa voidaan hyödyntää myös muutoin kuin tietoa siirtämällä; esimerkiksi tarjoamalla räätälöityjä “näkymiä” lähderekisteriin.
* Ns. palveluntarjoajan vaihtaminen on selkeä käyttötarve, esimerkiksi koulun vaihtaminen tai siirtyminen opiskelijaksi toiseen korkeakouluun.
* Rekisteröityminen vs. vahva tunnistautuminen; julkisen sektorin omadataa luovutetaan vain vahvasti tunnistautuneelle käyttäjälle, joten tämä voi vaikuttaa yksityisten palveluntarjoajien digitaalisten palveluiden toteutukseen.

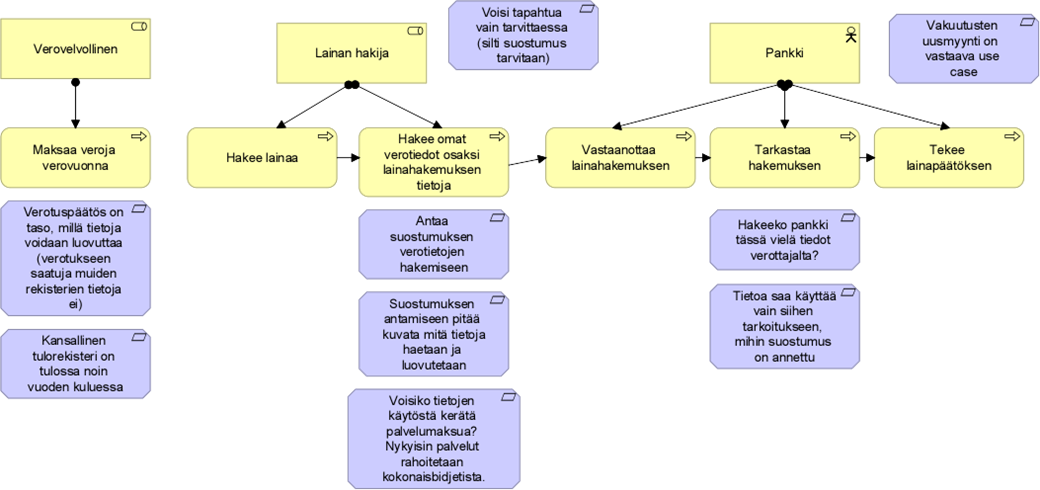
Opetus- ja kulttuuriministeriön hallinnonalalla on rakennettu kokoava tietovarantopalvelu (KOSKI-palvelu), jota voidaan hyödyntää keskitettynä omadatan lähteenä.

|  |
| --- |
| **Kansallisten opiskeluoikeuksien ja suoritusten keskitetty integraatiopalvelu KOSKI**  Koski on palvelu, jonka kautta julkisen valvonnan alaisen koulutuksen opinto-oikeus-, läsnäolo-, opintosuoritus- ja tutkintotiedot ovat keskitetysti kansalaisen nähtävissä ja käytettävissä. Henkilö voi palvelussa antaa suostumuksensa rekisterissä tai tietovarannossa olevan tiedon luovuttamiseen palvelun avulla muille tahoille. Palvelun avulla tietoja voidaan myös luovuttaa kattavasti, luotettavasti ja kustannustehokkaasti niitä toiminnassaan tarvitseville viranomaistoimijoille. Tietoa voidaan hyödyntää esimerkiksi opintojen suunnittelussa. Keskitetty suoritustieto helpottaa myös koulutukseen hakeutumista ja opitun tunnistamista ja tunnustamista. Uuden rekisterin avulla tiedot ovat helpommin käytettävissä rahoituksen laskennassa ja koulutuksen arvioinnissa. Tietolähteinä hyödynnetään jo olemassa olevia valtakunnallisia rekistereitä ja tietovarantoja, eli ylioppilastutkintorekisteriä, opiskelijavalintarekisteriä ja korkeakoulujen valtakunnallista tietovarantoa. Perusopetuksen ja toisen asteen koulutuksen tietoja varten ei toistaiseksi ole olemassa valtakunnallista tietovarantoa. Tämän vuoksi lailla perustetaan uusi tietovaranto näitä tietoja varten. Laki valtakunnallisista opinto- ja tutkintorekistereistä (ns. KOSKI-laki) astui voimaan 1.1.2018. |

### 

### Verotustietojen hyödyntäminen lainahakemuksessa

Verohallinnossa tunnistettiin kaksi käyttötapausta, joissa henkilöasiakkaalle voisi selkeästi olla hyötyä omien verotustietojen käytöstä. Tähän nostettiin niistä esimerkiksi toinen: asuntolainan hakeminen. Toinen käyttötapaus liittyy asunnon vuokraamisen ja sen tarkempi kuvaus löytyy liitteestä. Kannattaa kuitenkin huomioida, että tulevaisuudessa vastaavat tiedot voisi olla järkevämpää hakea keskitetystä kansallisesta tulorekisteristä.



Kuva 9. Verotustiedot osana verkossa täytettävää lainahakemusta.

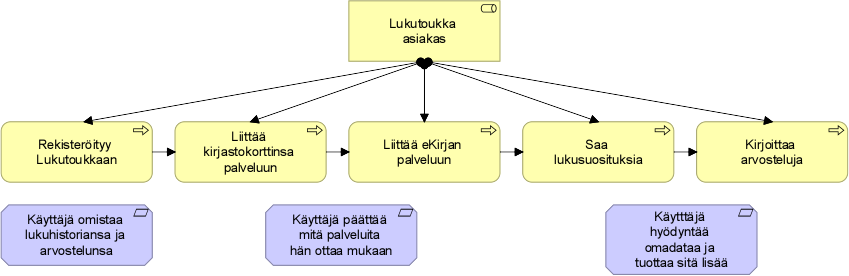
**Käyttötapausten kuvaamisen yhteydessä esiin nousseita vaatimuksia ja havaintoja:**

* Omadata -konseptilla ei voida korvata nykyistä massatiedonsiirtoa.
* Kaikki rekisterinpitäjällä oleva tieto ei välttämättä ole sellaista, jota voitaisiin luovuttaa omadatana. Verohallinnon tapauksessa selkeintä omadataa olisivat henkilön verotuspäätöksen tiedot (tiedot verifioitu Verohallinnossa)

### Minun Helsinki (Helsinki)

Helsingin kaupungin käyttötapauksiksi valittiin kaksi palveluprototyyppiä, jotka on ideoitu Helsingin kaupungin ja Open Knowledge Finland ry:n yhteisessä hankkeessa vuonna 2016.[[12]](#footnote-11)

Esimerkiksi valittiin tähän ns. Lukutoukka -palvelu.



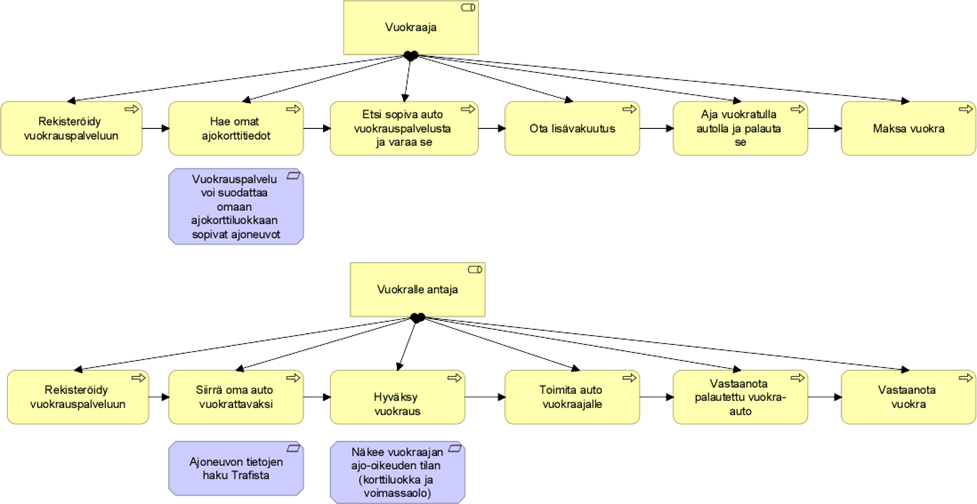
Kuva 10. Helsingin kaupungin kuvitteellinen Lukutoukka -palvelu.

**Käyttötapausten kuvaamisen yhteydessä esiin nousseita vaatimuksia ja havaintoja:**

* Osa kunnalle/kaupungille kertyvästä tiedosta on sellaista, että sitä voitaisiin yhdistää erilaisiin yksityisten toimijoiden tietoihin (kirjastosta lainatut kirjat & ostetut eKirjat). Tällöin henkilöllä itsellään voi olla myös merkittävä rooli tiedon tuottajana (lukusuositukset).
* Kunnassa / kaupungissa asumiseen ja palveluiden käyttämiseen liittyy erilaisia rooleja, joihin liittyy mm. erilaisia tunnistautumisen “vahvuusasteita” (asukkaan lupa-asiointi vs. satunnaisen kävijän käyttämät palvelut).
* Kunnan / kaupungin toimialojen välisessä tiedonvaihdossa on nykytilassa haasteita; jatkossa olisi järkevää pohtia joko lakisääteisen tiedonvaihdon kehittämistä tai suostumukseen perustuvaa tiedonvaihtoa silloin kuin lakisääteinen tiedonvaihto ei syystä tai toisesta ole mahdollista.
* Kunnan / kaupungin palveluiden tuottajina on moninaisia toimijoita, joiden rooli ei välttämättä selkeästi ole joko julkissektorin rekisterinpitäjä tai yksityinen rekisterinpitäjä. Näissä tapauksissa olisi tarpeen selkeyttää rooleja ja toimijoiden oikeuksia toimia lähderekistereinä tai tiedon vastaanottajina (esimerkiksi milloin on kyse tiedon ensisijaisesta käytöstä ja milloin toissijaisesta käytöstä).

### Ajoneuvon vertaisvuokrauspalvelu (Trafi)

Trafin osalta valittiin käyttötapaukseksi esimerkki, joka mahdollistaisi ajoneuvon vertaisvuokrauspalvelun toteuttamisen.



Kuva 11. Ajoneuvon vertaisvuokrauspalvelu

**Käyttötapausten kuvaamisen yhteydessä esiin nousseita vaatimuksia ja havaintoja:**

* Omadatalla ei korvata nykyistä tiedonvälitystä viranomaisten välillä.
* Keskitettyyn suostumusten hallintaan perustuvassa ratkaisussa hyödynnetään mahdollisimman pitkälle nykyisiä, olemassa olevia tiedonluovutusratkaisuja ja -kanavia ja suostumusten hallinnan rekisteri on keskitetty yhteen paikkaan.

## Vaiheen 2 edistyneet käyttötapaukset

Osa arkkitehtuurivisiossa tavoitelluista käyttötapauksista asettaa vaatimuksia, joita ei oleteta kokeiluvaiheessa olevan käytettävissä - kuten suostumustenhallintaa tarjoavien organisaatioiden luottamusverkosto, suostumuksen antaminen suoraan Hyödyntäjäpalvelussa tai lohkoketjuihin pohjautuvan hajautetun tilikirjan käyttö yleisenä omadata-infrastruktuurina. Käsittelystä notifiointi ja käsittelyn vastustaminen kuuluvat myös vaiheeseen 2.

Näistä tapauksista ei ole toiminta-arkkitehtuurin menetelmin tehtyä materiaalia, mutta niistä on kirjoitettu käyttötapauskuvaukset avaamaan konkreettisesti myöhemmän vaiheen mahdollistamia saumattomampia käyttäjäkokemuksia ja saavutettavissa olevaa lisäarvoa. Käyttötapauksien lisäksi on otettu esiin myös yleisen tietosuoja-asetuksen asettamia velvoitteita ja rajauksia.

### Suostumuksen antaminen ja hallinta Hyödyntäjäpalvelussa

“Liisa on hakemassa itselleen uutta yksilöityä terveysvakuutusta omasta vakuutusyhtiöstään. Vakuutusyhtiön verkkoportaali kertoo, että voidakseen antaa sitovan vakuutustarjouksen ja ehdotuksen räätälöidystä bonustarjouksesta, heidän on saatava tietoonsa Liisan viimeisen viiden vuoden hoitohistoria julkisesta ja yksityisestä terveydenhuollosta, joiden asiakas Liisa on ollut aiemmin. Vakuutusyhtiö on kerännyt mahdolliset palveluntarjoajat osaksi palvelunäkymää, jossa Liisalta pyydetään suostumuksia näihin eri palveluissa sijaitseviin tietoihin. Koska Liisa ei ole vielä tunnistautunut hakemuspalveluun, pitää hänen tässä kohtaa tunnistautua vakuutusyhtiön portaalissa omilla pankkitunnuksillaan. Tämän jälkeen Liisa voi valita listalta itseensä sopivat palveluntarjoajat, joista kustakin esitetään pyydetyt tiedot ja käsittelyn tarkoitus suostumuksen antamista varten. Liisa kuittaa suostumukset voimaan käymättä koskaan vakuutusyhtiön palvelun ulkopuolella.”

“Kahta vuotta myöhemmin Liisa on ottanut käyttöönsä älypuhelimessa toimivan uuden tunnuslompakko-sovelluksen. Käyttöönotossa Liisalle on tarjottu mahdollisuus siirtää kaikki voimassa olevat suostumuksensa lompakkoon, josta käsin hän nyt aina pystyy hallinnoimaan itsestään tarjolla olevia verifioituja lupa-, koulutus- ja pätevyystietoja ja avaamaan pääsyn tietoihin eri palveluille. Lupatietojen välitys tapahtuu tietoturvallisesti palvelujen ja Liisan oman tunnuslompakon välillä ja voimassaolevat luvat ja tiedonsiirtosuostumukset ovat todennettavissa tarvittaessa lohkoketjuihin perustuvalta julkiselta tilikirjalta joka sijaitsee hajautettuna ympäri maailmaa. Liisa ei tuosta halunnut tietää yhtään enempää kuin että se toimii luotettavasti ja kaikki liittyy hänen uuteen kätevään sähköiseen identiteettiinsä, joka sidottiin sitä luodessa hänen tuttuun vanhaan *Suomi.fi*-tunnistautumisessa käytettävään vahvasti tunnistettuun identiteettiin.”

### Notifiointi ja henkilötietojen käsittelyn läpinäkyvyys

“Liisa sai tunnuslompakko-sovellukseensa loppiaisen jälkeen viestin, jossa kerrottiin hänen vuosittain koostettavan tietotilinpäätöksensä olevan tarjolla. Liisa sai viestissä kertakäyttöisen web-linkin, jonka kautta hän pääsee katselemaan henkilötietojensa viimeisen 12 kuukauden ajalla tapahtunutta käsittelyä eri viranomaisrekistereissä ja hänen itse luvittamissaan muissa palveluissa. Raportti näkyy Liisan *Suomi.fi*-palvelujen ‘Tietosuojani ja tietojen käyttö’ -osiossa ja sen voi ladata halutessaan omalle laitteelle PDF-muodossa. Liisa on kuitenkin todennut tämän tarpeettomaksi, tietotilinpäätökset säilyvät *Suomi.fi*:ssä ja tarjoaapa joku kumppanipalvelu myös tilinpäätösten analyysiä ja vertailua tarjoavan palvelun, jonne tietotilinpäätöksensä voi luvittaa toimitettavaksi automaattisesti.”

|  |
| --- |
| Huomioitavaa: Notifioitavien, samoin kuin suostumukseen perustuvien tietosiirtojen lokittaminen on erityisesti Lähdepalvelujen vastuulla, ja on siis huomioitava aina palvelun paikallisessa toteutuksessa. Suostumustenhallintapalvelu ei lokita muita kuin suostumusten antamiseen tai poistamiseen liittyviä lokitietoja. Notifiointi tietosiirroista tehdään palvelun toimesta kansalaisen ‘omadata-tilille’ - joka voi ottaa joskus tulevaisuudessa myös jonkinlaisen lupalompakko-sovelluksen muodon.  Yleinen tietosuoja-asetus ja siihen liittyvä vuoden 2017 lopussa julkaistu [tulkintaohjeistus](http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850) ohjaa läpinäkyvyyden toteuttamisesta erityisesti tietosuojaselosteiden laatimisen ja tietopyyntöihin liittyvän soveltamisen osalta. |

### Henkilötietojen käsittelyn vastustaminen

“Pekka näkee viimevuotisen tietotilinpäätöksensä sivulta, että hänen kiinteistö- ja maanomistustietojaan on toimitettu Maanmittauslaitoksen viranomaisten sisäisen käsittelyn lisäksi automaattisesti myös heidän kumppanipalveluilleen, joiden omistajaprofiloinnin mainitsevia tiedon käsittelytarkoituksia hän ei tunnistanut tarkemmin asiaan tutustuttuaan kannaltaan oleellisiksi.

Pekka pureutuu palvelunäkymässä tämän tietosektorin hyödyntäjäpalvelujen palvelukuvauksiin, ja ilmaisee vastustuksensa tiedon toimittamisesta näiden palveluntarjoajien käyttöön Maanmittauslaitoksen toimesta. Hän valitsee ao. palveluntarjoajien kohdalla valikosta vaihtoehdon ‘En halua tietojani käsiteltävän tässä palvelussa’. “

|  |
| --- |
| Huomioitavaa: Lakisääteisissä ensisijaiseen käsittelyyn liittyvissä julkishallinnon palveluissa käsittelyn vastustamisoikeutta ei useimmiten voi toteuttaa.  Vastustamisoikeus on kuvattu TsA §21:  “*1. Rekisteröidyllä on oikeus henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä, joka perustuu 6 artiklan 1 kohdan e tai f alakohtaan\*, kuten näihin säännöksiin perustuvaa profilointia. Rekisterinpitäjä ei saa enää käsitellä henkilötietoja, paitsi jos rekisterinpitäjä voi osoittaa, että käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy, joka syrjäyttää rekisteröidyn edut, oikeudet ja vapaudet tai jos se on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi.*  *2. Jos henkilötietoja käsitellään suoramarkkinointia varten, rekisteröidyllä on oikeus milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä tällaista markkinointia varten, mukaan lukien profilointia silloin kun se liittyy tällaiseen suoramarkkinointiin.*  *3. Jos rekisteröity vastustaa henkilötietojen käsittelyä suoramarkkinointia varten, niitä ei saa enää käsitellä tähän tarkoitukseen.*  *4. Viimeistään silloin, kun rekisteröityyn ollaan yhteydessä ensimmäisen kerran, 1 ja 2 kohdassa tarkoitettu oikeus on nimenomaisesti saatettava rekisteröidyn tietoon ja esitettävä selkeästi ja muusta tiedotuksesta erillään.*  *5. Tietoyhteiskunnan palvelujen käyttämisen yhteydessä ja sen estämättä, mitä direktiivissä 2002/58/EY määrätään, rekisteröity voi käyttää vastustamisoikeuttaan automaattisesti teknisiä ominaisuuksia hyödyntäen.*  *6. Jos henkilötietoja käsitellään tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten 89 artiklan 1 kohdan mukaisesti, rekisteröidyllä on oikeus henkilökohtaiseen tilanteeseensa liittyvällä perusteella vastustaa häntä itseään koskevien henkilötietojen käsittelyä, paitsi jos käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi.”* |

|  |
| --- |
| \*TSA §6 alakohta 1. e) käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi; 1.f) käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi…  Ensimmäisen alakohdan f alakohtaa ei sovelleta tietojenkäsittelyyn, jota viranomaiset suorittavat tehtäviensä yhteydessä. |

# 

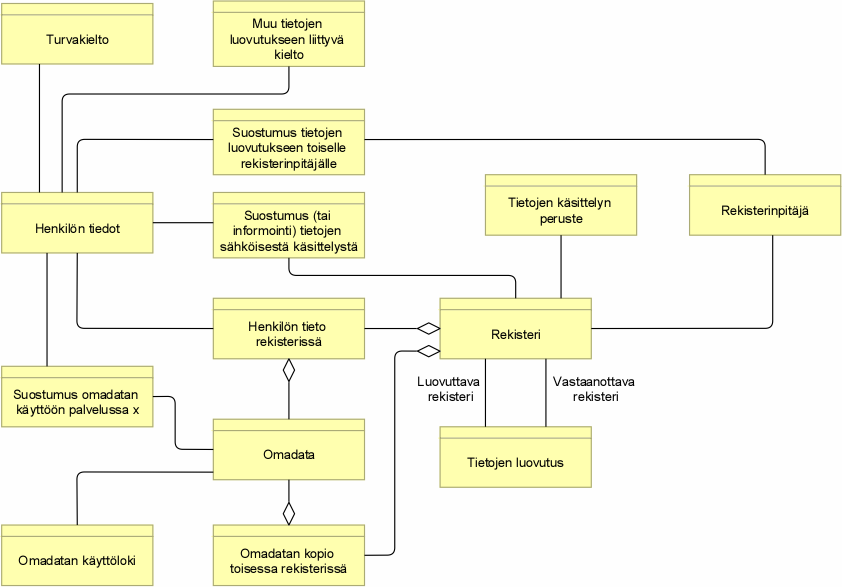
# Tietoarkkitehtuuri

Suostumustenhallinnan arkkitehtuurille oleellisiksi tietoarkkitehtuurilinjauksiksi on tunnistettu seuraavat:

* Suostumustallenne on uusi, rekisteröidyn luvittaman tiedonsiirron laajuuden tarkasti rajaava tietorakenne.
* Tallenne syntyy tuloksena dialogista käyttäjän ja suostumusta pyytävän asiointipalvelun välillä.
* Suostumusehdotusten rakentaminen asiointipalveluissa ja suostumusten kirjaaminen vaatii palveluilta koneluettavia metatietoja, kuten palvelukuvauksia ja kuvaukset tiedoista ja rajapinnoista mitä halutaan luvitettaviksi.
* Henkilötietojen käytöstä käyttäjälle notifioiminen tarvitsee oman tieto- ja käsittelykuvauksen notifikaatioiden lähdeaineistoksi (tuotetaan myöhemmin).
* Metatietokuvausten rakenteet ovat erilaisia riippuen siitä onko kyseessä tietoja luovuttava vai hyödyntävä palvelu/organisaatio
  + luovuttava palvelu kuvaa erityisesti luvitettavat tiedot - MITÄ
  + hyödyntävä palvelu kuvaa MIKSI se tarvitsee rekisteröidyn tietoja.
* Kuvausten koostaminen ja toimittaminen on sekä lähde- että hyödyntäjäorganisaatioden vastuulla.
* Suostumuksella saatua henkilön omadataa ei voi siirtää eteenpäin kolmannelle osapuolelle eli ns. tiedonluovutuksen ketjutus ei ole sallittua ilman henkilön nimenomaista suostumusta.
* Omadatan luovuttaminen henkilön itsensä tai hänen luvittamansa palvelun käyttöön ei tarkoita sitä, että kyseinen tieto poistuisi lakisääteisestä rekisteristä. Henkilötieto jää edelleen rekisterinpitäjän haltuun ja ylläpidettäväksi sen alkuperäisen käyttötarkoituksen mukaisesti. Rekisterinpitäjän rooli tietojen hallinnointivastuullisena säilyy tiedon alkuperäisen version osalta.

## Käsitemalli

Omadatan käytölle rekistereissä on kuvattavissa kuvan 12 mukainen käsitemalli.



Kuva 12. Omadata käsitemallina

Käsitemallin selvennykset:

Kullakin *Rekisterillä* on *Rekisterinpitäjä*. Rekisterinpitäjä vastaa rekisterin tietosisällöstä ja tietojen oikeellisuudesta.

Rekisterissä voi olla henkilöiden tietoja (*Henkilön tieto rekisterissä*), osa näistä tiedoista on *omadataa*, osa rekisterinpitäjän keräämää muuta henkilöön liittyvää tietoa.

Rekisteristä toiseen voidaan tehdä *Tietojen luovutus*. Luovutus voi perustua lakiin tai siitä voidaan pyytää erillinen suostumus.

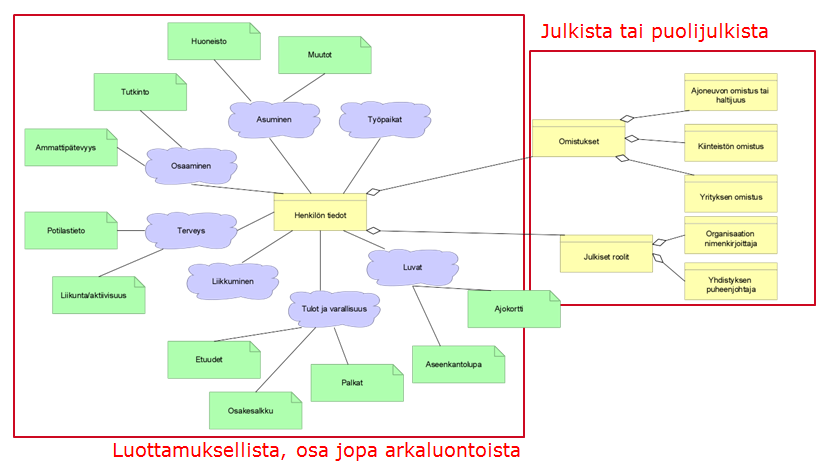
Jos tietoja on kopioitu rekisteristä toiseen (tietojen luovutuksen yhteydessä) ja teknisistä syistä tiedoista on päädytty tekemään kopio, eivät kopioidut tiedot kuitenkaan muutu vastaanottavan rekisterin ”omistamiksi” vaan alkuperäisen rekisterinpitäjän rooli tietojen pääasiallisena hallinnointivastuullisena säilyy.

Henkilöiltä voidaan pyytää suostumuksia tietojen luovuttamiseen ja sähköiseen käsittelyyn. Omadata tarvitsee oman suostumusmekanismin (*Suostumus omadatan käyttöön palvelussa x*).

Henkilöllä voi olla *Turvakielto*. Lisäksi henkilö on voinut asettaa *Muita tietojen luovutukseen liittyviä kieltoja*. Nämä ovat erilaisia eri toimialoilla, mm. terveydenhuollossa on omat määrittelyt kieltojen osalta.

## Omadataan liittyvät tiedot ja tietomallit

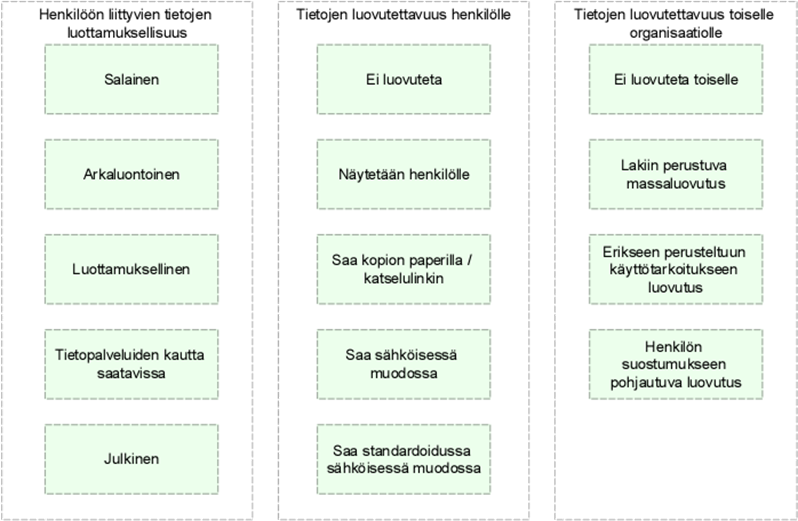
Tässä luvussa kuvataan omadata-palvelujen tarjoamiseen ja hyödyntämiseen liittyvät tiedot ja tietovarannot. Omadataa tarjoavien tai hyödyntävien asiointipalveluiden osalta kuvataan niiden palvelu- ja tietokuvauksiin liittyvät järjestelmät ja käytännöt.



Kuva 13. Henkilöön liittyvää, potentiaalista omadataa.

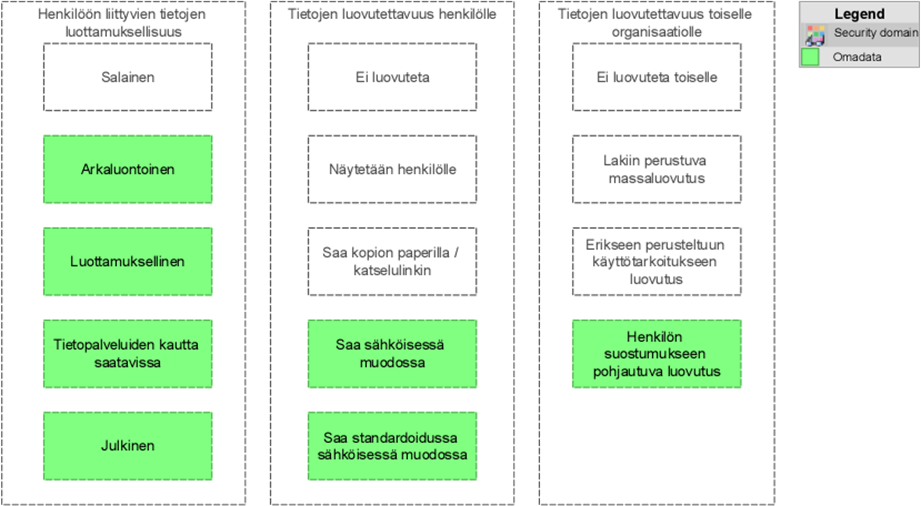
Yllä olevaan kuvaan on hahmoteltu erilaisia tietokokonaisuuksia, jotka ovat potentiaalista omadataa. Tiedot ovat nykyisen lainsäädännön perusteella luokiteltavissa erilaisiin “julkisuusasteisiin”. Kuva ei ole kattava, vaan julkissektorin organisaatioiden olisi itse tunnistettava, kuvattava ja luokiteltava rekistereissään oleva henkilöön liittyvä tieto ja potentiaalinen omadatana hyödynnettävissä oleva tieto.

Luokittelussa on huomioitava useita näkökulmia, joten ennen tunnistamis- ja kuvaamistyötä olisi pohdittava tarvittava metatietomalli eli mitä kaikkia attribuutteja metatietoihin kannattaa sisällyttää jotta voidaan tunnistaa henkilöasiakkaille tarjottava omadata.



Kuva 14. Näkökulmia tietojen luokitteluun.

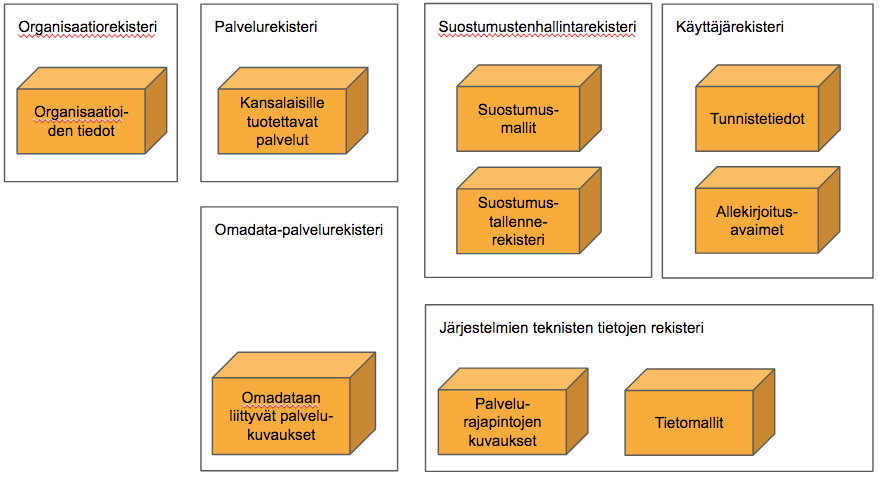
Omadataa ovat todennäköiset sellaiset tiedot tai tietokokonaisuudet, jotka täyttävät useita tunnusmerkkejä. Alla luonnos erilaisista vaatimuksista ja edellytyksistä.



Kuva 15. Potentiaalisia omadatan ominaispiirteitä

### Loogiset tietovarannot

Alla on kuvattu visuaalisesti rekisterien looginen jaottelu omadata-arkkitehtuurissa osoittamatta niitä vielä osaksi nykyisiä kohdearkkitehtuureja ja niiden jo olemassa olevia rekistereitä ja varantoja. Tavoitetilan vaatiman työn projektoinnin yhteydessä tämä järjestely voi muuttua.



Kuva 16. Suostumustenhallinnan yhteydessä tarvittavia loogisia rekistereitä. Suostumusten- hallintapalvelun rekisteri ja omadata-palvelurekisteri ovat uusia kokonaisuuksia.

### Tietovirrat

Esitetyissä tietovirtakaavioissa on kirjattu tietojen siirtyminen kahdessa eri toiminnallisessa prosessissa: 1) palvelujen ilmoittaminen ja rekisteröinti Omadata-palvelurekisteriin ja 2) operatiivinen suostumusten käsittely suostumustenhallintapalvelussa sen saadessa suostumuspyynnön asiointipalvelulta.

# 

Kuva 17. Tietovirrat palvelujen rekisteröinnissä/ilmoittamisessa (nykyiset samannimiset, olemassaolevat palvelut vaativat kehittämistä virtojen mahdollistamiseksi).

Palvelun rekisteröinti (ilmoittaminen) tapahtuu visioidusti Palveluhallinnan soveltuvassa näkymässä, jossa

1. kerätään palvelun oleelliset kuvaukset ja
2. ne siirretään omadata-metatietorekisteriin ja ihmiseluettavat palvelukuvaukset sisältävään Palvelutietovarantoon.
3. Lähderekisterien omadata-rajapintojen tietojen tulee olla saatavilla myös Liityntäkatalogin kautta.
4. Yhteentoimivuusvälineistöä hyödynnetään tarjoamalla olemassaolevia tietomäärityksiä kehittäjille tiedoksi ja mahdollistetaan uusien tietotyyppien lisääminen.

(Näistä vain Palvelutietovarannon tiedot vastaanottava rajapinta ja Yhteentoimivuusvälineistö ovat työkaluina olemassa, muiden osalta tarvitaan muutoksia tai täysin uusi kokonaisuus.)

# 

Kuva 18. Tietovirrat operatiivisessa suostumuspyyntötilanteessa. Suostumustieto toimitetaan myös sitä pyytäneelle asiointipalvelulle (ei kuvassa).

# Tietojärjestelmäarkkitehtuuri

Tässä osiossa kuvataan oleelliset suostumusten hallinnassa käytettäviin tai siihen operatiivisten käyttötapausten kautta integroituviin sidosarkkitehtuureihin liittyvät tietojärjestelmävaatimukset ja -rakenteet. Asiakirjan liitteissä esitetään myös muutamia suostumustenhallinnan tyypillisten käyttötapausten prosessikaavioita (katso esim. [liite 3](#_47cl6nfjci8v)).

Notifiointipalvelun ja henkilökäsittelyn vastustamisen vaatimukset täydennetään myöhemmässä vaiheessa.

Osio on muun dokumentin mukaisesti jaoteltu vaiheen 1 ratkaisuun omadata-palvelupilotteja varten ja tavoitetilan visioon (vaihe 2). Yleiskäyttöisten palvelujen osalta tarvittavat komponentit ja palvelut on ajateltu toteutettaviksi yhteisenä infrastruktuurina - esimerkiksi Suomi.fi-palvelujen kautta.

## Suostumustenhallinta palveluna

Suostumustenhallinnan tavoitetilassa omadata-palveluihin liittyvät käyttäjien suostumukset hallinnoidaan infrastruktuuripalveluna, jota voidaan käyttää hajautetusti suostumustenhallinnan omaan luottamusverkostoon kuuluvissa palveluissa. Tietojärjestelmätasolla muodostetaan julkishallinnon rekisterinpitäjien käytettäväksi suostumusrekisteristä huolehtiva uudelleenkäytettävä palvelu. Vaiheessa 1 haetaan kokemuksia hajauttamiseen ja keskittämiseen perustuvista järjestelmäarkkitehtuureista. Vaihe 2 visioi suostumustenhallinnan lähtökohtaisesti täysin hajautettua toteuttamista hyödyntämällä esimerkiksi hajautettujen julkisten tilikirjojen teknologiaa.

Yksilöivät suostumukset tallennetaan palvelun avulla koneluettavassa muodossa rekisteriin - tästä tallennusdokumentista käytetään tässä arkkitehtuurissa nimeä suostumustallenne (engl. consent record). Tallenne on aina käyttäjäkohtainen, eli käytännössä rekisteri koostaa yhteen kaikkien ao. palveluilmentymässä omadataa luvittaneiden käyttäjien antamat suostumukset.

Suostumusrekisterin palvelu- ja järjestelmätason toiminnasta vastaa sen liiketoimintalogiikan sisältävä kone (engl. engine). Kone huolehtii myös suostumusten hallintaan liittyvistä osaprosesseista: suostumusehdotuksen koostaminen palvelua hyödyntäviä käyttäjänäkymiä varten, käyttäjän tekemän suostumuksen kirjaaminen ja sähköinen allekirjoittaminen, suostumuksen tilaan tai ehtoihin liittyviin kyselyihin tai toimintapyyntöihin reagointi ja suostumusten päivittäminen tai revokointi eli poisvetäminen.

## Suostumustenhallinta-infrastruktuuripalveluskenaariot (Vaihe 1)

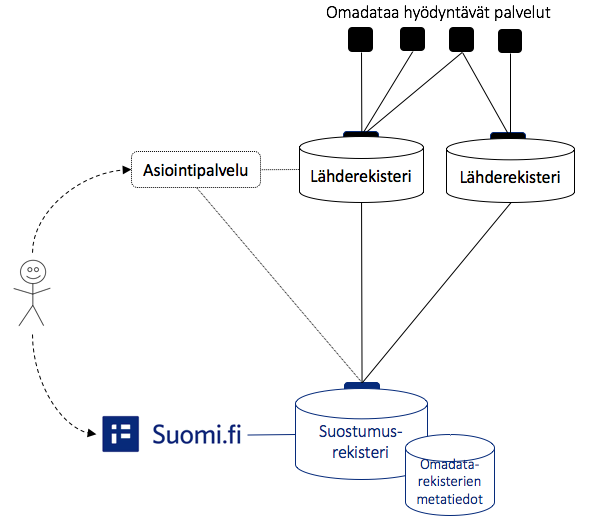
Kuten mainittu aiemmin, vaiheen 1 suostumustenhallinta ja muut omadataan liittyvät yhteiset palvelut on tarkoitus toteuttaa ainakin osin yhteisenä infrastruktuurina Suomi.fi palveluportfolion kautta. Tulevissa luvuissa kuvataan skenaarioiden kautta, miten Suomi.fi-palveluita voitaisiin hyödyntää. Valittava toteutustapa tarkennetaan Yhteinen tiedon hallinta -hankkeen työn edetessä.

### Keskitetty suostumustenhallinta

Suomi.fi-palveluja maksimaalisesti hyödyntävän skenaarion mukaisesti kaikki julkishallinnon Omadata-suostumukset säilytetään ja hallinnoidaan keskitetyn ratkaisun avulla, jossa

* Julkishallinnolla on keskitetty Omadata-suostumusrekisteri, joka perustuu Lähderekisterien omistajien tuottamiin metatietokuvauksiin.
* Käyttäjä voi tarkastella Lähdepalvelujen tietoja Suomi.fi-palvelussa rekisterinäkymänä eli tietoja ei tallenneta/kopioida Suomi.fi-palveluun.
* Lisäksi sektori tai virasto voi tarjota oman asiointipalvelun, jonka kautta Lähderekisterin/-palvelun tietoja voi tarkastella.
* Käyttäjä hallinnoi omia suostumuksiaan Suomi.fi-palvelussa. Lisäksi sektori tai virasto voi tarjota oman **asiointipalvelun**, jonka kautta tietojen omistaja voi hallita ko. Lähderekisteriin/-palveluun liittyviä suostumuksia. Paikallinen asiointipalvelu tallentaa suostumukset ja muutokset keskitettyyn rekisteriin eikä muodosta omaa kopiota rekisteristä.
* Tietojen luovutus niitä hyödyntäville palveluille tapahtuu sektori- tai virastokohtaisista palveluista/rekistereistä. Lähderekisteri tarkistaa luovutuspyynnön saatuaan keskitetystä Suostumusrekisteristä, onko ko. palvelulla oikeus pyydettyihin tietoihin.
* Suostumusrekisterin rekisterinpitäjänä toimii keskitetyn ratkaisun tuottaja.

Tämä skenaario on hahmoteltu kuvassa 19.

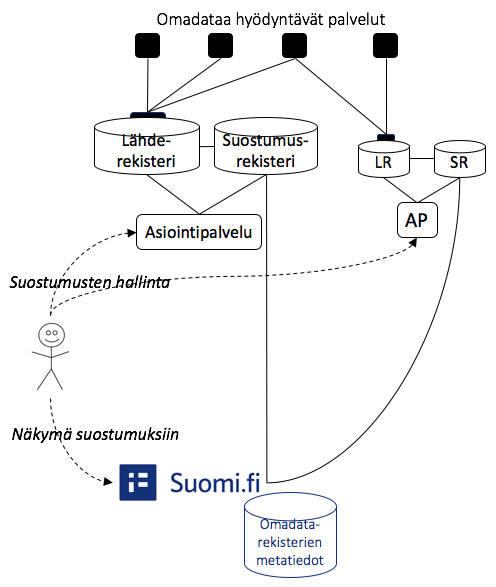


Kuva 19. Keskitetty suostumustenhallinta -vaihtoehto.

### 

### Hajautettu sektorikohtainen suostumustenhallinta

Hajautetussa skenaariossa julkishallinnon suostumukset säilytetään ja hallinnoidaan sektori- tai virastokohtaisissa ratkaisuissa, ja Käyttäjälle tarjotaan lisäksi keskitetty näkymä kaikkiin suostumuksiin Suomi.fi-palvelun kautta (hahmotelma kuvassa 20).



Kuva 20. Virastokohtainen, hajautettu suostumustenhallinta.

Tässä skenaariossa julkishallinnon omadataa soveltavat virastot tai sektorit tuottavat omat suostumustenhallintaratkaisut, jotka sisältävät

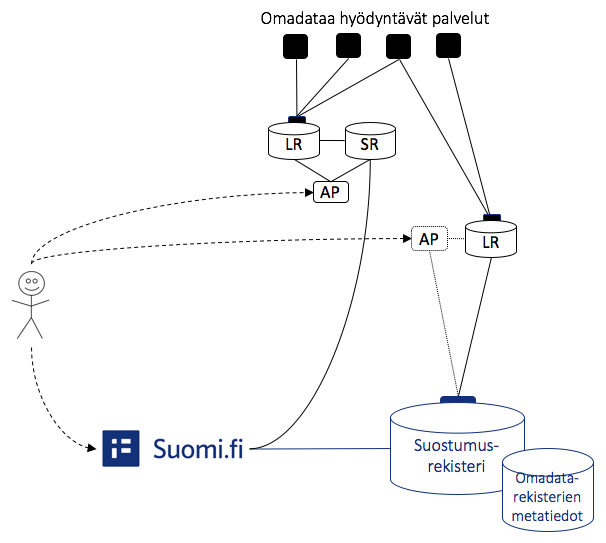
* suostumusrekisterin,
* asiointipalvelun, jonka kautta tietojen omistaja katselee ja hallinnoi omia ko. viraston/sektorin lähdetietoihin liittyviä suostumuksiaan ja
* rajapinnan, jonka kautta suostumustietoja on mahdollista kysyä keskitettyyn näkymään Suomi.fi-palveluun. Kaikkien virastojen/sektorien rajapinnat ovat yhdenmukaiset (käytetään yhteistä rajapinnan toteuttavaa ohjelmistokomponenttia ja sen versiota).

Tietojen omistaja voi katsella kaikkia julkishallinnon Omadata-suostumuksia keskitetyn näkymän kautta Suomi.fi-palvelun rekisterinäkymän kautta. Suomi.fi-palvelu ohjaa käyttäjän hallinnoimaan suostumuksia viraston/sektorin asiointipalveluun.

Suostumusrekisterien rekisterinpitäjänä toimii aina virasto tai sektori, jonka hallinnoimasta lähdeaineistosta on kyse.

### Hybridimallinen suostumustenhallinta

Kolmannessa ns. hybridiskenaariossa julkishallinnon suostumuksia varten perustetaan keskitetty hallintapalvelu ja suostumusrekisteri. Tästä huolimatta sektori tai virasto voi halutessaan toteuttaa myös oman suostumustenhallintaratkaisun (hallintapalvelun ja suostumusrekisterin), mutta on tässä tapauksessa velvoitettu tuottamaan myös rajapinnan, joka mahdollistaa vähintään näkymän sektorikohtaisessa hallintapalvelussa hallinnoitaviin suostumuksiin myös keskitetyssä palvelussa. Arkkitehtuuri on hahmoteltu kuvassa 21.



Kuva 21. Suostumustenhallinnan hybridimalli, jossa on sekä keskitetty että sektorikohtaisia suostumusrekistereitä ja yhteinen omadataa tarjoavien rekisterien metatietorekisteri.

Tietojen omistaja voi katsella kaikkia julkishallinnon Omadata-suostumuksia keskitetyn näkymän kautta Suomi.fi-palvelussa. Jos virasto/sektori on toteuttanut oman suostumustenhallintaratkaisun, ohjataan käyttäjä hallinnoimaan suostumuksiaan ko. palveluun – muussa tapauksessa vaihtoehdosta 2 poiketen hallinnointi tapahtuu Suomi.fi-palvelussa. Teknisesti tämän toteuttaminen tarkoittaisi ao. lähderekisterin rajapinnan suostumuksista vastaavan SH-ilmentymän rekisteröintiä osana metatietoja (vain yksi mahdollinen).

* Keskitettyä suostumusratkaisua hyödyntävä virasto/sektori voi halutessaan tuottaa asiointipalvelun, jonka kautta käyttäjä voi myös katsella ja hallinnoida näitä suostumuksiaan – suostumukset tallennetaan kuitenkin tässäkin tapauksessa keskitettyyn rekisteriin.
* Keskitettyyn suostumusrekisteriin tallennetaan vain ne suostumukset, joita ei ylläpidetä virasto-/sektorikohtaisissa rekistereissä – **yksittäinen suostumus tallennetaan vain yhteen paikkaan**.

Suostumusrekisterin rekisterinpitäjänä toimii ratkaisusta riippuen virasto-/sektorikohtaisen suostumusrekisterin omistaja tai keskitetyn ratkaisun tuottaja.

Kaikissa kolmessa lähestymistavassa Lähderekisterin omistajat kuvaavat omadataa tarjoavan rekisterin keskitettyyn ratkaisuun, josta muodostuu Omadata-rekisterien metatietokuvaukset sisältävä rekisteri. Metatietoihin perustuen on mahdollista tuottaa palvelu, jonka kautta tietoja hyödyntävät tai niistä kiinnostuneet tahot saavat keskitetysti tiedot kaikista julkishallinnon Omadataa tarjoavista Lähderekistereistä.

Tietojen luovutus niitä hyödyntäville palveluille tapahtuu aina sektori- tai virastokohtaisista palveluista/rekistereistä. Lähderekisteri tarkistaa lähestymistavasta riippuen joko keskitetystä tai virasto-/sektorikohtaisesta suostumusrekisteristä, onko ko. Hyödyntäjäpalvelulla oikeus pyydettyihin tietoihin.

## Avainvaatimukset

**Suostumustenhallintapalvelun** on riippumatta sovellettavasta järjestelmäarkkitehtuurimallista (keskitetty, hajautettu tai hybridi) mahdollistettava:

1. löydettävyys tarjoamalla suostumustenhallintapalvelun omat metatiedot, esimerkiksi julkisen .well\_known/mydata/ URI:n kautta
2. suostumusehdotusten koostaminen suostumustenhallintanäkymissä Lähde- ja Hyödyntäjäpalvelujen Omadata-palvelurekisteriin ilmoittamien metatietojen (koneluettavien palvelukuvausten) perusteella
3. käyttäjän suostumuksen dokumentointi suostumuksen antohetkellä (mitkä tiedot käyttäjä luvittaa ja mille ajanjaksolle, mistä Lähdepalvelusta tieto on sovittu siirrettäväksi ja mikä on kohteena oleva Hyödyntäjäpalvelu)
4. suostumustallenteen allekirjoitus käyttäjän allekirjoitusavaimella
5. tukemilleen omadata-palveluille ja niiden käyttäjille yhteisen suostumusrekisterin hallinnointi
6. käyttäjien allekirjoitusavainten tietoturvallinen hallinnointi (PKI)
7. käyttäjäkohtaisten suostumustallenteiden listaus ja näyttäminen yksityiskohtineen (esim. näyttämään tarkasti yksittäiset tai listaamaan kaikki lokitietoineen)
8. em. tietojen pyynnöstä toimittaminen ohjelmointirajapinnan kautta luotetuille suostumustenhallintanäkymille tai palvelun paikalliselle suostumustenhallinta-asiakkaalle
9. käyttäjäkohtaisen suostumushistorian lokittaminen, ja myöhemmin koko rekisterin tasoinen tilastollinen kerääminen

**Lähderekistereihin/-palveluihin** kohdistuvat avainvaatimukset tietojärjestelmätasolla ovat:

1. Suostumustenhallinnalle alisteisten tietojen ja niitä tarjoavien ohjelmistorajapintojen järjestäminen kokonaisuudeksi, joka toimii yhteen suostumustenhallintapalvelun määriteltyjen rajapintojen kanssa.
2. Lähderekisterin omadata-rajapinnalle käyttämän suostumustenhallintapalvelun tunnistaminen (oma tai keskitetty)
3. Em. tietojen kirjaaminen Omadata-palvelurekisterin metatietokuvauksiksi ja näiden kuvausten aktiivinen ylläpitäminen.
4. Tietoja luovuttavien ohjelmistorajapintojen ja resurssijoukkojen kuvausten tarjoaminen joko ‘hajautetusti’ osana omaa palvelua (oman palvelun .well\_known/mydata/ URI:n[[13]](#footnote-12) takana) tai rekisteröinti ao. toiminnon tarjoavassa palvelussa jolla hallinnoidaan omadata-metatietorekisteriä.
5. Hyödyntäjäpalvelujen tiedonsiirtotapahtumien lokittaminen.

**Hyödyntäjäpalveluihin** kohdistuvat avainvaatimukset tietojärjestelmätasolla ovat:

1. Suostumukseen perustuvien pyydettävien tietojen metatietojen kirjaaminen Omadata-palvelurekisteriin. Toimitukseen kuuluu tietomallien ja tietojen käsittelytarkoituksien kuvaaminen ja palvelun oman julkisen avaimen ja palvelinsertifikaatin kirjaaminen tietoturvallisen kommunikoinnin mahdollistamiseksi. Rekisterin kautta näiden metatietojen ylläpitämisen vaihtoehto on kuvausten ylläpitäminen omana julkisesti löydettävissä olevana .well\_known/mydata -resurssina.
2. Määritellä em. ilmoittautumisen yhteydessä käsittelytarkoituskohtaisen suostumuksen tietovaatimukset eli (tieto)resurssit, jotka ovat palvelulle välttämättömiä tarjotun lisäarvopalvelun tuottamiseksi.
3. Täyttää tekniset luottamusverkoston sääntöjen asettamat vaatimukset, kuten käyttää suostumuksenhallinnan tai lähdepalveluiden välisessä tiedonsiirrossa omaa Omadata-palvelurekisteriltä saatua palvelutunnistetta ja -sertifikaattia.
4. Allekirjoittaa suostumustenhallintarajapintaan lähetetyt rajapintakutsut omalla allekirjoitusavaimellaan.

|  |
| --- |
| Huomioitavaa: Suostumukseen perustuvien tietosiirtojen lokittaminen on erityisesti Lähdepalveluiden vastuulla, ja on siis huomioitava aina palvelun paikallisessa toteutuksessa. Suostumustenhallintapalvelu ei lokita muita kuin suostumusten antamiseen tai pois vetämiseen liittyviä paikallisia lokitietoja - eli se ei ole tietoinen tapahtuneista tiedonsiirroista, jollei se saa näitä tietoja esimerkiksi Lähdepalvelulta erikseen määriteltävän notifiointirajapinnan kautta. |

## Suostumustenhallintapalvelun komponentit

Tässä luvussa avataan visioidun yleiskäyttöisen suostumustenhallintapalvelun ja sitä hyödyntävien asiointipalvelujen yksityiskohtaisempia suunnittelu- ja integraatiorakenteita.

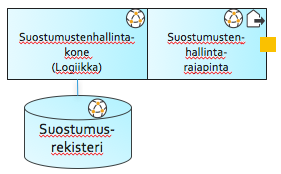
Suostumustenhallinnan tulisi olla itsenäinen mikropalvelu, joka tarjoaa ohjelmistorajapinnat joilla voidaan toteuttaa loppukäyttäjille hallintanäkymiä ja mahdollistaa suostumuksiin liittyvien transaktioiden tekemisen itsensä ja luotettujen Lähde- tai Hyödyntäjäpalvelujen tietojärjestelmien välillä (kuva 22). Ulospäin mikropalvelu näkyy näille em. asiakkaille suostumusten hallinnan mahdollistavana yleiskäyttöisenä ohjelmallisena rajapintana (API:na).

Joissakin kuvissa on käytetty *Suomi.fi-suostumukset* työnimeä ja puhutaan keskitetystä näkymästä. Arkkitehtuuriratkaisu on mikropalveluna kuitenkin yleiskäyttöinen eli sopii myös hajautetun sektorikohtaisen suostumustenhallintapalvelun pohjaksi.

### Hallintalogiikka

**Suostumustenhallintalogiikka** on sisäinen komponentti, joka käsittelee suostumusten kontrollilogiikkaa ja kerää tai tallentaa tietoja suostumuksiin ja palveluihin liittyen. Se allekirjoittaa suostumustallenteet hallussaan olevalla käyttäjän yksityisellä kryptografisella avaimella, ja kirjaa ne suostumusrekisteriin. Logiikkakomponentti järjestäisi todennäköisesti myös suostumuksien tilamuutoksiin ja käyttöön liittyvän lokittamisen.

**Suostumusrekisteri** on edellisen komponentin omistama sisäinen tietovaranto, joka ylläpitää suostumustallenteita kullekin käyttäjälle. Ulkoiset omadata-palvelujen kyselyt tai muut tapahtumapyynnöt rekisterin suostumuksiin kanavoidaan aina suostumustenhallinnan rajapinnan kautta.

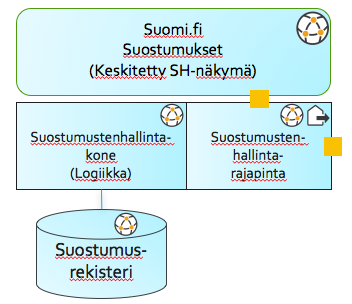


Kuva 22. Suostumustenhallinta-mikropalvelun komponentit ilman asiointinäkymän toteuttamisesta vastaavaa sovelluskomponenttia.

### Hallintanäkymä

Kansalaiselle näkyvä asiointipalvelun **suostumustenhallintanäkymä** käyttäisi yllä kuvattua mikropalvelua aina sen julkisen API-rajapinnan kautta. Näkymä voidaan räätälöidä (kontekstualisoida) rajapintakutsun parametrien perusteella osoittamaan näkymän käyttäjälle näyttämässä suostumusehdotuksessa esim. valmiiksi haettuun suostumukseen liittyvät palvelujen tiedot ja palvelukuvaukset ja suostumuksen laajuuteen liittyvät valinnat/vaihtoehdot.

Vaiheessa 1 suostumustenhallintanäkymä voitaisiin tarjota keskitetyn asiointipalvelun kautta, kontekstualisoituna suostumuspyynnön yksityiskohtiin (kuva 23). Tämä ratkaisu ei taivu toteuttamaan suostumuspyynnön käynnistävän palvelun omaa brändiasua eikä täysin saumatonta käyttäjäkokemusta samassa sovellusikkunassa, tai ns. natiivisovelluksessa jos kyse olisi mobiilisovelluksista.



Kuva 23. Keskitetyistä julkishallinnon suostumuksista vastaavan *Suomi.fi*-suostumustenhallinnan avainkomponentit

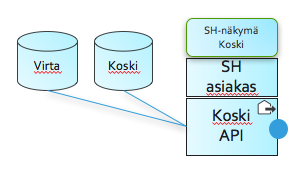
Vaiheessa 2, luottamusverkoston toiminnan vakiinnuttua ja tietojärjestelmäkomponenttien teknisen kypsymisen jälkeen, suostumustenhallinnan käyttöliittymänäkymiä voitaisiin toteuttaa myös muiden palvelunäkymien kautta - oleellista on, että näkymät tarjotaan/isännöidään ekosysteemin luotetuista palveluista tai appseista. Lähde- ja erityisesti Hyödyntäjäpalvelujen itse tarjoamat suostumusehdotuksen esittävät käyttöliittymänäkymät ovat käyttäjäkokemuksen perspektiivistä toivottavia, mutta asettavat toteutuksissaan tiukan haasteen palvelujen luotettavuudelle. Riski tietojen päätymisestä ei-tarkoituksenmukaiseen käyttöön kasvaa, jos erikseen säännöillä sidottu luottamusverkosto ei kontrolloi esimerkiksi hyödyntäjäpalvelujen todellista tietojen käyttöä metatiedoissa ja julkisessa tietosuojaselosteessa ilmoitettuja käyttötarkoituksia vasten. Luottamusverkoston jäsenten kesken sallituista toimintatavoista ja sanktioinnista tulisi sopia sopimusten kautta. Myöhemmässä vaiheessa tietojen kolmansille osapuolille siirtymisen seuranta (ns. data provenance) on myös ehkä teknisesti toteutettavissa kirjaamalla siirtotapahtumat hajautettuun, julkiseen tilikirjapalveluun.

Palvelujen omien suostumustenhallintanäkymien käyttö mahdollistettaisiin rekisteröimällä sopimuksin sidotuille tai muuten luotetuille palvelinpohjaisille asiointipalveluille tarvittavat suostumustenhallintapalvelun rajapinta-avaimet ja/tai sitomalla mobiilisovellukset (suostumustenhallinta-asiakkaat) suostumustenhallintapalveluun dynaamisesti sovelluksen käyttöönotossa ja rekisteröinnissä. Jälkimmäisellä tavalla toimii esimerkiksi Omatietovarannon mobiilisovellusten dynaaminen rekisteröinti sen OAuth-autorisointipalvelinta vasten[[14]](#footnote-13).

### Rajapinta-asiakas

Lähderekisterin, Hyödyntäjäpalvelun tai rinnakkaisen suostumuksenhallintapalvelun oma asiointipalvelu käyttää yksittäisen suostumustenhallintapalvelun rajapintapalvelua erillisen **suostumustenhallinta-asiakkaan** ilmentymän (kuvassa 24 näkyvä *SH-asiakas*) kautta. Tämä komponentti toimii paikallisena liiketoimintalogiikkana joka esimerkiksi ilmoittaa palvelun paikalliselle autorisointilogiikalle (kuten Palveluväylän Liityntäpalvelin liitetyn palvelun SOAP-kutsujen autorisointipalvelimena, tai Web-rajapinnan tapauksessa esim. resurssien autorisointia hallinnoiva OAuth-palvelin), mitkä Käyttäjän tunnisteeseen liittyvistä tiedoista Lähdepalvelun rajapinnassa voidaan toimittaa Hyödyntäjäpalvelulle tämän niitä sen kautta pyytäessä.

Ensimmäisissä omadata-piloteissa ehdotetaan suostumustenhallinnan käyttäjänäkymäksi yleisvaatimuksissa aiemmin kuvattua kontekstualisoitua (Lähdepalvelulta rajapintakutsussa saatujen tietojen perusteella räätälöityä) näkymää. Tämän tarjoaisi *Su0mi.fi*-verkkopalvelu sen oman selainikkunan tai -tabin kautta.



Kuva 24. Lähdepalvelu rekistereineen, rajapintoineen ja ulkoiseen mikropalveluun tukeutuva suostumuksenhallinta-asiakas. Ylinnä mahdollinen rekisterin oman asiointipalvelun hallintanäkymä (kuvassa esimerkkinä OPH:n Koski).

|  |
| --- |
| **Suostumus autorisoinnin rajaajana**  Autorisointia pyydettyihin tietoihin voidaan rajoittaa Suostumusrekisteriin tallennetun suostumuksen osoittamien, käyttäjän tietoisesti tekemien rajausten perusteella. Nämä riippuvat käyttäjän henkilökohtaisista valinnoista suostumusehdotuksen hyväksynnän yhteydessä.  Kuitenkaan valinnaisuutta tietotyyppien osalta ei ole pakko (eikä välttämättä mielekästä hyödyntäjäpalvelun tarvenäkökulmasta) tarjota yksittäiseen käyttötarkoitukseen kohdistuvan suostumusehdotuksen sisällä, ks. TsA:n mukaisten suostumusten toteuttamiseen luotu lisäohjeistus joulukuulta 2017[[15]](#footnote-14).  Monimuotoisemmissa suostumusehdotuksissa (joissa esimerkiksi aggregoidaan useampi käyttötarkoitus ja siihen sidottu tietojoukko yhteen ehdotusnäkymään) rajaukset käyttäjänäkymässä pitää sallia - yksittäiselle käyttötarkoitukselle (ja sen tiedoille) joko myönnetään suostumus tai ei. |

|  |
| --- |
| **Autorisoinnin keskittäminen**  Lähdepalvelu voisi teoriassa ‘alihankkia’ myös paikallisen rajapinnan autorisoinnin yhteiseltä palvelulta, jolloin sen rooliksi jäisi vastata rajapinnoistaan autorisoitavissa olevien tietojen (ns. resurssien ja resurssijoukkojen) rekisteröinnistä keskitetylle autorisointipalvelulle operatiivista luvittamista varten. OAuth-autorisoinnin tälle on mietitty käyttötapauksia teollisuudessa ja se on mahdollista jos käytössä olisi ns. [federoitu autorisointipalvelu](https://docs.kantarainitiative.org/uma/wg/oauth-uma-federated-authz-2.0-05.html) (UMA 2.0). UMA-profiilin mukainen autorisointipalvelu toimisi keskitettynä infrastruktuuripalveluna, suostumustenhallinnasta vastaavan infrastruktuuripalvelun rinnalla. Tähän liittyisi Palveluhallinnan tuottama resurssien rekisteröintirajapinta. |

### Suostumustallenne

**Suostumustallenne** on koneluettava tietue, johon tallennetaan suostumuksen dokumentoivat tiedot. Tallenne tulisi kiistämättömyyden osoittamiseksi luontihetkellä allekirjoittaa vähintään käyttäjän yksityisellä avaimella, mahdollisesti myös Suostumustenhallintapalvelun omalla avaimella.

Suostumuksen perusteella rajapinnasta luettavissa olevat tiedot on yksilöitävä yksikäsitteisesti. Ne voidaan yksilöidä tallenteen sisäisessä alirakenteessa esimerkiksi ns. **Resurssijoukolla** (engl. resource set) joka on määritelty mm. MyData-viitearkkitehtuurin suostumustenhallintaa käsittelevässä dokumentissa[[16]](#footnote-15).

Luvitettavan resurssijoukon määrittävät tietorakenteet on kuvattu allaolevassa taulussa - käytännön toteutus on suositeltavaa tehdä esim. JSON-objektirakenteiden avulla:

*Taulu 3: Resurssijoukon tunniste*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| rs\_id | Source URI || Resource Key   |  |  | | --- | --- | | Source URI | Lähdepalvelun yksilöivä URI | | Resource Key | Lähdepalvelun sisäinen, suostumukseen kuuluvan resurssijoukon yksilöivä tunniste/avain | |

*Taulu 4: Resurssijoukko*

|  |  |
| --- | --- |
| rs\_id | Resurssijoukon tunniste |
| resurssi [1..n] | |  |  | | --- | --- | | resource\_id | Resurssin tunniste (\_id) palvelun tietokuvauksesta | | distribution\_id | Resurssin jakelutunniste (distribution ID), haetaan Lähdepalvelun datakuvaukset sisältävän objektin sisällöstä. *Ei käytetä jos suostumus liittyy vain palvelun sisäiseen käyttöön.* | | distribution\_url | Host || Service access URI || Distribution URI  *Ei käytetä jos suostumus liittyy vain palvelun sisäiseen käyttöön.*   |  |  | | --- | --- | | Host | Palvelun tarjoavan palvelininstanssin domainnimi | | Service Access URI | Palveluinstanssin tarjoaman käyttörajapinnan URI | | Distribution URI | Resurssin rajapinnassa jakeleva URI | | |

Suostumustallenne on mm. edellä kuvattua resurssijoukon käsitettä koneluettavassa muodossa esitettävä tietue, jonka mahdollinen rakenne[[17]](#footnote-16) on kuvattu allaolevassa taulussa 5 (toteutus taas JSON-rakenteena).

*Taulu 5: Tiedon toissijaiseen käyttöön annettava suostumustallenne*

|  |  |  |
| --- | --- | --- |
| **Avain** | **Tyyppi** | **Kuvaus** |
| **Yhteinen osio** | | |
| version | String | Käytetyn suostumustallennemallin versionumero |
| cr\_id | String | Tallenteen yksilöivä tunniste |
| surrogate\_id | String | Suostumuksen antavan Käyttäjän ns. Sijaistunniste. Käytetään jos suostumusta pyytävä palvelu on pitänyt lisätä (linkittää) Käyttäjän käytössä olevaan Suostumuksenhallintapalveluun. |
| rs\_description | Object | Suostumuksen kattaman resurssijoukon kuvaava objekti |
| slr\_id | String | Ns. Palvelulinkkitallenteen yksilöivä tunniste (jos palvelun linkitystä on käytetty) |
| service\_description\_version | String | Suostumuksen voimaan astuessa käytetyn Hyödyntäjäpalvelun palvelukuvauksen versionumero |
| consent\_proposal | Object | |  |  | | --- | --- | | **Avain** | **Kuvaus** | | url | Käyttäjälle näytetyn suostumusehdotuksen URL | | hash | Suostumusehdotuksen SHA-256 sekoite | |
| iat | Integer | Suostumuksen myöntämishetki |
| nbf | Integer | Aika: suostumuksen voimassaolon takaraja (not valid before) |
| exp | Integer | Aika: suostumuksen viimeinen voimassaoloaika (expiration) |
| operator | String | Suostumustallenteen luoneen suostumustenhallintapalvelun yksilöivä tunniste |
| subject\_id | String | Suostumuksen saaneen Hyödyntäjäpalvelun yksilöivä palvelutunniste |
| pop\_key | JWK | Hyödyntäjäpalvelun allekirjoittaman käyttötunnussanoman (‘proof of possession token’) julkinen avain JWK-muodossa. JWK:n on sisällettävä ‘kid’ parametri. |
| rs\_id | String | Lähdepalvelusta suostumuksen perusteella luettavissa olevan resurssijoukon yksilöivä tunniste |
| usage\_rule | Object | |  |  | | --- | --- | | **Avain** | **Kuvaus** | | purposeId | Suostumukseen liittyvän Käyttökuvauksen tunniste | |

Tallenteen olemassaolo on oltava tarkistettavissa Suostumustenhallintapalvelun rajapinnasta tarvittaessa myös Hyödyntäjäpalvelun aloitteesta (jos/kun Hyödyntäjäpalvelu tarvitsee suoran todisteen voimassaolevasta suostumuksesta).

Tämän voi mahdollistaa toimittamalla Suostumustenhallintapalvelun vastauksessa Lähdepalvelulta tulleeseen pyyntöön 1) myönnetyn suostumuksen ja 2) myöntäneen suostumustenhallintapalvelun tunnisteet. Ensimmäinen on oltava paikallisesti, jälkimmäinen yleisesti yksikäsitteinen. Nämä tiedot voidaan toimittaa edelleen Hyödyntäjäpalvelulle esimerkiksi Lähdepalvelun myöntämän käyttötunnussanoman (kuten OAuthin Access Token) osana/mukana.

Vaiheessa 1 nämä viitetiedot toimivat Hyödyntäjän tositteena suostumuksen myönnöstä.

Vaihe 2 mukainen järjestelmien kypsyystaso mahdollistaa suostumuksen tilan tarkistamisen (kuten myös tallenteen luomisen) suoraan Hyödyntäjäpalvelun ja Suostumustenhallintapalvelun välillä.

|  |
| --- |
| **Poikkeamat alkuperäisestä MyData-arkkitehtuurikehyksestä**  Tunniste on alkuperäisessä asiakirjan muutamaan otteen viittaamassa MyData-viitearkkitehtuurikehyksessä ajateltu luotavaksi erikseen Lähde- ja Hyödyntäjäpalvelulle jaettavaksi erisisältöisinä versioina, pääosin tietosuojan ylläpitämiseksi. Alkuperäisestä konseptista poiketen tallenteen rakenne yksinkertaistuu jos:  1) Suostumusrekisteriin talletetun tallenteen tiedoista vain osa toimitettaisiin Lähdepalvelun Suostumuksenhallinta-asiakkaalle (ja edelleen rajanpinnan pääsyä kontrolloivalle autorisoinninhallinnalle) tiedoksi, ja  2) luovutaan mahdollisuudesta antaa Käyttäjälle valinnanmahdollisuus luvitettavan tietojoukon atomisten tietotyyppien osalta.  Selventäen:   * Myönnetty suostumus kattaa näin aina *kaikki* tiedot mitä käyttötarkoituskohtainen tietotyyppien listaus (resurssijoukko) Hyödyntäjäpalvelun omadata-palvelurekisteriin ilmoittamassa palvelukuvauksessa sisältää. * Hyödyntäjäpalvelu voi hyödyntää vain resursseja, joihin se on itse rekisteröitynyt käyttäjäksi ao. Lähderekisterin rajapinnan osalta. Tätä rekisteröintiä varten oletetaan Liityntäkatalogin tai Lähdepalvelujen itse tai (vaiheessa 2) laajennetun palveluhallintakokonaisuuden tarjoavan tarvittavat API-rekisteröintitoiminnot kuten rekisteröintiä varten dedikoitu rekisteröintirajapinta tai -rekisteröintiportaali. |

|  |
| --- |
| **Hybridiarkkitehtuurin toteutuksesta tietojärjestelmäkomponenteilla**  Jos virastot halutessaan toteuttavat oman palveluilmentymän paikallisille suostumuksille (eli lähestytään yhteentoimivaa suostumustenhallintaratkaisua joustavalla hybridiarkkitehtuurilla), itse paikallisen ilmentymän tekninen toteutus on samanlainen poislukien näkymien suunnittelu ja muu asiointipalvelun integraatioon liittyvä lisätyö.  Hybridimallissa yksittäisen kansalaisen kaikkien voimassaolevien suostumusten kerääminen hajautetuista palveluista esim. Suomi.fi-palvelunäkymäksi olisi mahdollista jos ylläpidetään operatiivisten ‘operaattorien’ suostumustenhallintapalvelurekisteriä (virtuaalista tai keskitettyä) ja käyttäjä identifioidaan kaikissa palveluissa samalla virtuaalitunnisteella. Tämä mahdollistaa suostumusten kokonaisuuden keräämisen tunnetuista mahdollisista rajapinnoista, ja yksittäisten suostumusten tilan muuttamisen.  Suostumustenhallinnan yleiskäyttöisten ohjelmistokomponenttien hallinta tulisi tässä tapauksessa osoittaa jollekin taholle, joka pystyy suorittamaan järjestelmien versio- ja ylläpidon hallintaa yli kaikkien virastojen IT-hallinnon. |

## Suostumuksenhallinnan ohjelmistorajapinnat (APIt)

Palvelu on tarkoitus toteuttaa mikropalveluna, joka yleisesti tarkoittaa sen toiminnallisuuksien käyttöä sille määriteltyjen ohjelmallisten rajapintojen kautta. Infrastruktuuritasolla toimivaa palvelukomponenttia voidaan käyttää eri palvelukokonaisuuksissa integroimalla se esimerkiksi suostumusta pyytävän tai suostumuksen voimassaolon tarkistamisesta vastuullisen asiointipalvelunäkymän omaan logiikkaan.

Myös integraatio ja kommunikaatio esimerkiksi rinnakkaisten suostumustenhallintapalveluiden kesken (useampi ‘omadata-operaattori’ ja käyttäjän suostumusten siirto tai välittäminen niiden välillä) tarvitsee rajapinnan.

Suostumustenhallinnan ja sitä kertakirjautumisen (engl. single sign-on, SSO) avulla tunnistusfederaation sisällä kutsuvien palvelujen tulee identifioida käyttäjä yhteisellä tunnisteella. **Henkilötunnuksen käyttöä ao. tunnisteena tulisi välttää.** Kun käyttäjä kirjautuu vahvan Suomi.fi-tunnistuksen kautta, käyttäjälle tulee luoda tietoturvallisesti palvelukohtainen virtuaalitunniste (pseudonyymi) joka toimii jatkossa palvelun suuntaan käyttäjän yksilöivänä tunnisteena.

Jos keskenään kommunikoivat palvelut käyttävät Käyttäjästä eri tunnistetta, tulee tunnisteet suostumustenhallintaa käyttävässä Lähdepalvelussa ja Suostumustenhallintapalvelussa (jälkimmäisessä käyttäjä on Suomi.fi-tunnistettu) assosioida toisiinsa. Tähän on käytetty esim. MyData arkkitehtuurikehyksessä ns. palvelun linkitystä[[18]](#footnote-17) (engl. Service Linking), jolla on oma ohjelmallinen rajapintansa. Käyttäjän tunniste toisessa palvelussa assosioidaan sijaistunnisteen (engl. surrogate ID) avulla.

Alle on luonnosteltu karkealla tasolla suostumustenhallintapalvelun toteuttamisessa oleelliset rajapinnat ja niiden perusresurssit/kutsut. Itse lopullisia teknisiä rajapintakuvauksia ei esitetä, sillä tekniset määrittelyt Suomi.fi-palveluväylän REST-rajapinnoille luodaan vasta 2018 aikana. Samanaikaisesti tarvitaan vastaavat SOAP-rajapintamäärittelyt liityntäpalvelinten ja suostumustenhallintapalvelun väliseen kommunikointiin.

|  |
| --- |
| Hyödyntäjäpalvelujen ja käyttäjien tunnistamisesta ja autorisoinnista Palveluväylässä määritellään Suomi.fi-palveluväylän viitearkkitehtuurin Liitteessä 3[[19]](#footnote-18) (kappale 2.1). Viitearkkitehtuurissa noudatetaan toistaiseksi näitä suosituksia julkishallinnon palvelujen osalta.  Omadata-palvelujen rekisteröinnissä voidaan harkita luottamusverkoston hallittua teknistä laajentamista soveltamalla nykymallisen VRK-varmenteiden käytön lisäksi myös palveluntarjoajan ns. ‘holder-of-key’ avaimen julkisen avaimen rekisteröintiä. Näin kommunikaatiossa voitaisiin käyttää palvelun avaimella allekirjoitettuja ja suostumuksenhallintapalvelun avattavissa olevia REST-rajapintakutsuja. Tämä vaihtoehto on tarpeen jos rajapintaa käyttävä palvelu ei ole kytketty Suomi.fi-palveluväylään liityntäpalvelimella. |

Suostumuksenhallinta-API:

* *Suostumuksen statuskysely* (hyödyntäjäpalvelun tunniste, lähderekisterin tunniste, käyttäjän tunniste)
  + Vastaa onko parametrien rajaamalla kokonaisuudella aiempi suostumus vai ei.
  + Vastaus: kyllä (suostumuksen tunniste) / ei / poisvedetty / virheilmoitus
* *Suostumupyyntö* (hyödyntäjäpalvelun tunniste, lähderekisterin tunniste, käyttäjän tunniste, käsittelytarkoituksen tunniste)
  + Kutsulla pyydetään suorittamaan SH-palvelua suorittamaan suostumuspyyntö parametrien rajaamalle kokonaisuudelle.
  + Vastaus: 200 OK (suostumuksen tunniste) / ei suostumusta / virheilmoitus
* *Poista suostumus* (suostumuksen tunniste)
  + Asettaa tunnisteen määrittämän suostumuksen tilan poisvedetyksi.
  + Vastaus: 200 OK / virheilmoitus
* *Toimita suostumusmalli* (hyödyntäjäpalvelun tunniste, lähderekisterin tunniste)
  + Toimittaa asiointinäkymässä visualisoitavan suostumusesityksen tarvitsemat koneluettavat tiedot
  + Vastaus: suostumusmallin tiedot / virheilmoitus
* *Käyttäjän suostumukset* (käyttäjän tunniste)
  + Listaa käyttäjän suostumusrekisteristä löytyvät suostumukset
  + Vastaus: lista(suostumustallenne1,...,suostumustallenneN)

Suostumustilin hallinta-API:

* *Luo tili* (käyttäjän tunniste)
  + Luo suostumustenhallintapalvelussa uuden tyhjän käyttäjäkohtaisen tilin ja käyttäjäavaimen.
  + Vastaus: 200 OK (käyttäjätunniste) / virheilmoitus
* *Poista tili* (käyttäjän tunniste)
  + Poistaa suostumustenhallintapalvelussa ao. käyttäjätunnisteen käytössä olleen tilin.
  + Vastaus: 200 OK / virheilmoitus
* *Tuo tili* (käyttäjän tunniste)
  + Siirtää vastaanottavassa suostumustenhallintapalvelussa ao. käyttäjän tunnisteen käytössä olleen tilin ja siihen liittyvät linkkitallenteet kutsuvaan suostumustenhallintapalveluun.
  + Vastaus: 200 OK / virheilmoitus

Palvelun linkittämisen API:

* *Yhdistä palvelu* (palvelun tunniste, käyttäjän tunniste)
  + Luo yhteyden Käyttäjän omadataa käyttävän palvelun ja SH-palvelun välille ja sitoo käyttäjätunnisteet palveluissa -> ‘linkkitallenne’.
  + Vastaus: 200 OK (linkkitallenteen tunniste) / virheilmoitus
* *Poista palvelu* ((linkkitallenteen tunniste)
  + Poistaa yhteyden Käyttäjän omadataa käyttävän palvelun ja SH-palvelun väliltä.
  + Vastaus: 200 OK / siirretty (käyttäjän uuden SH-palvelun tunniste) / virheilmoitus

## 

## 

## Suostumustenhallinnan tavoitetila (Vaihe 2)

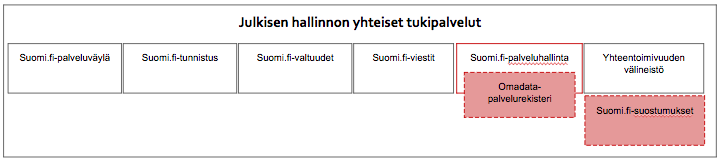
Tavoite on, että ensimmäisen vaiheen kokeilujen ja komponenttien kehittämistyön kautta kehitetty suostumustenhallinta kehittyy joustavaksi palvelukomponentiksi:

* Julkishallinnon palvelukartalla suostumustenhallinta on yhteinen tukipalvelu, jota voidaan käyttää joustavasti eri palvelujen toimintojen osana, samaan tapaan kuin tunnistautuminen tai puolesta-asiointi jo nyt mahdollistaa.
* Käytettävyydeltään optimoituja hallintanäkymiä voidaan luoda luotettujen verkko- tai mobiilipalvelujen omiin käyttöliittymiin.
* Tietojen luvittaminen suostumusten kautta voidaan sitoa hierarkkisesti käyttäjän yksilöiviin erilaisiin digitaalisiin tunnisteisiin ja niihin liittyviin tunnistautumisen luottamustasoihin.
* Suostumustenhallinta voidaan myös mahdollisesti toteuttaa täysin hajautettuna ratkaisuna sopivalla hajautettuihin tilikirjateknologioihin tukeutuvalla ratkaisulla.
* Kaikkea tietoa ei tarvitse identifioida, luvittaa ja siirtää järjestelmien välillä käyttäjän vahvan tunnistamisen kautta, koska käyttäjät tunnistetaan julkishallinnossa yhteisellä yksilöivällä ainutlaatuisella tunnisteella (UUID, Universally Unique IDentifier). Operatiivisissa järjestelmissä käytettävä tunniste ei ole nykyinen henkilötunnus.

Näistä tavoitteista tai toteutustavoista on kustakin alla kirjatuissa kappaleissa tarkempi selvitys. Tavoitetilan *Suomi.fi*-palveluiden käyttö on visioita eikä niiden esittäminen sido palveluja hallinnoivaa Väestörekisterikeskusta valmistelun tässä vaiheessa.

### Yhteinen palvelu julkishallinnon palvelukartalla

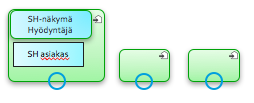
JHKA-palvelukartalla (Julkisen hallinnon kokonaisarkkitehtuuri) visioitu Omadata-infrastruktuuri sijoittuu yhteisten tukipalvelujen osioon nykyisten Viestien, Valtuuksien ja Tunnistus -palvelujen rinnalle. Omadata-metatietorekisteri on osa Palveluhallinnan kokonaisuutta ja Suostumukset olisi uusi kansalaisen asiointipalvelu (kuva 21):



Kuva 25. Palvelukartan yhteiset tukipalvelut

### Luvitusnäkymät luotetuissa Hyödyntäjäpalveluissa

Suostumuksen kysyminen alun perin lupaa tiedon hakemiseen pyytävässä sähköisessä palvelussa - ilman siirtymisiä Suostumustenhallintapalvelun ja alkuperäisen asiointipalvelun näkymien välillä - on saumattoman käyttäjäkokemuksen ydin. Tämä on mahdollista toteuttaa tietoturvallisesti arkkitehtuurissa, jossa suostumuspyyntö rakennetaan esimerkiksi Hyödyntäjäpalvelun palvelunäkymän logiikassa (kuva 22) hyödyntäen tietoja, jotka ovat saatavilla luvitettavista palveluista itsestään (kuten palvelukuvausten metatiedot) ja ao. palveluun linkitetyn suostumustenhallintapalvelun rajapinnan kautta.



Kuva 26. Suostumustenhallinta (logiikka ja asiointipalvelu/käyttäjänäkymä) osana tietoja pyytävää Hyödyntäjäpalvelua.

Käyttäjiä tahallisesti harhaanjohtavien suostumusehdotusten välttämiseksi suostumuksen tallentaminen, vaihtoehtoista tietä todentaminen (“Hyväksyinkö oikeasti sen mitä luulin hyväksyväni?”) ja kryptografinen allekirjoittaminen tulisi edelleen tehdä paikassa, jossa on käytössä Käyttäjän ja Suostumustenhallintapalvelun allekirjoitusavaimet - Lähderekisterin ilmoittamassa suostumustenhallintapalvelussa.

Suostumustenhallintanäkymien osalta hajautettu ratkaisu vaatii palvelujen välille sekä teknisesti että sopimuksellisesti tiukan luottamusverkoston. Paikallisten hallintanäkymien toteutusten käytettävyyden kannalta ‘best practices’ tyyppiselle toteutusohjeistukselle on todennäköisesti tarvetta.

Mahdolliset muut Käyttäjän luottamusta asiointitapahtumassa lisäävät elementit, kuten esim. omadata-luottamusverkostoon kuulumisesta kertova näkyvä leima/ikoni osana näkymää tmv., kannattaa harkita osaksi käyttöliittymätoteutusten ohjeistusta, jos tällaisia elementtejä tulee aikanaan saataville. Näitä ei ole odotettavissa aivan lähitulevaisuudessa, koska esim. EU-komission toimesta tietosuoja-asetuksen toteuttamisen helpottamiseksi tarkoitettuja ikoneja tullaan tutkimaan vaikuttavuusanalyysiä hyödyntävien, laajojen kokeilujen kautta.

### Identiteetin luottamustasot ja suostumus eri tiedoille

Kansalaiskäyttäjän toimenpiteiden kirjaaminen tunnistettuna on julkishallinnon palveluissa toistaiseksi mahdollista vain vahvalla Suomi.fi-tunnistautumisella ja siihen liitetyillä pankkitunnuksilla ja Mobiilivarmenteella. Näiden ns. luotettavuustaso (engl. level of assurance, LoA) on 4/3 (operaattori & pankkitunnuksilla 3) ja näin henkilö voidaan tunnistaa palveluissa luotettavasti. Tietotyyppikohtaiseen luvittamiseen ei toistaiseksi ole Suomessa tarjolla vaihtoehtoisia tunnistautumistekniikoita, eikä eri tiedoille ole asetettu eritasoisia tunnistautumisen varmuustasoja.

|  |
| --- |
| Esimerkiksi: henkilön opiskelijastatus voisi tietona olla vähemmän arkaluontoinen tai pienemmän riskin omaava tieto, ja sille voisi asettaa alemman tunnistautumisen varmuustason kuten LoA 2. Näin opiskelijastatusta pyytävässä palvelussa ja samoin suostumuksia hallinnoivassa palvelussa voisi käyttää LoA 2 -tason tunnistautumista, joka käytettävyydeltään voi olla ratkaisevasti parempi käyttötilanteesta ja -laitteesta riippuen. |

Tietojen luvittamiseen tulisikin palvelujen kehittäjien tai tuottajien näkökulmasta tietojen kuvausprosessin yhteyteen tuoda tarjolle rajattu skaala mahdollisia tiedonsiirron luvittamiseen kelpaavia tunnistautumisen varmuustasoja. Asiointipalveluissa voi olla käytettäviä osioita, joissa ei tarvita vahvaa tunnistautumista, ja esimerkiksi vain arkaluontoisia tietoja omadata-palveluille luvitettaessa tai pyydettäessä Käyttäjän pitäisi tunnistautua vahvemmin. Englanninkielinen yleisesti käytetty termi tälle toimintatavalle digitaalisissa palvelupoluissa on ‘*step-up authentication*’.

USA:ssa NIST:in aikanaan määrittelemä ja yleisesti identiteettien hallinnassa käytetty LoA-käsite häviää ja tilalle tulee koko liittovaltion tasolla käyttöön otettava kolmitasoinen järjestelmä (tarkemmin: [SP 800-63-3](https://pages.nist.gov/800-63-3/)), jossa määritellään eri käsitteinä toiminnallinen

* Identiteetin varmuustaso IAL
* käyttäjän tunnistamisprosessin (identity proofing) taso AAL
* tunnistautumisratkaisun ns. federoinnin varmuustaso FAL

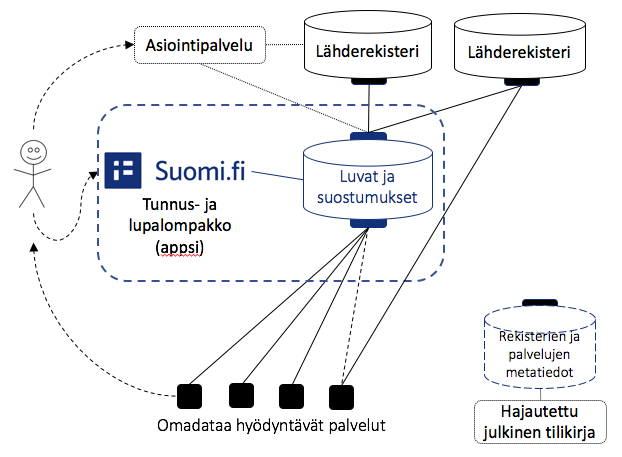
NIST:in julkaisema uusi malli levinnee ennen pitkää myös Eurooppaan ja kannattaa siis ottaa huomioon Suomi.fi-tunnistuksen omalla tiekartalla.

### Hajautetut tilikirjateknologiat suostumustenhallinnassa

Hajautettujen tilikirjaratkaisujen (engl. *DLT, Decentralised Ledger Technology*) kuten uPort, Sovrin, Civic ym. päätyessä mahdollisesti käyttöön julkishallinnossa identiteetin- ja suostumustenhallinta ja arkkitehtuurimallit saattavat muuttua radikaalisti: perinteinen vahvasti tunnistettu, keskitettyyn identiteetintuottajaan tai identiteetin toimittajien federaatioon perustuva nykymuotoinen sähköinen identiteetti saa rinnalleen hajauttamiseen perustuvan identiteettitunnisteen, ‘riippumattoman identiteetin’ (engl. *self-sovereign identity*). Keskitettyä identiteetin toimittavaa auktoriteettia ei ole, eikä henkilölle luotua identiteettiä voida ottaa yksilöltä pois, ja sitä voi lähtökohtaisesti käyttää missä tahansa ilman maantieteellisä rajoitteita, jos sovellettu tilikirjaratkaisu on käytössä globaalisti. Tunnisteelle voidaan luoda luottamustaso luomalla (allekirjoittamalla ja kirjoittamalla julkiseen tilikirjaan) hajautettu identiteetti erityisen tilikirjaverkostoon kytketyn solmun, ns. luottamusankkurin toimesta. Valtionhallinnossa esimerkiksi Väestörekisterikeskus, nykymuotoisten henkilötunnusten myöntäjä, voisi toimia hajautetussa, globaalissa verkossa yhtenä luottamusankkurina. Tunnuksia voidaan luoda sekä luonnollisille että oikeushenkilöille (kuten yritykset tai julkishallinnon organisaatiot).

Riippumattoman identiteetin mallissa jokainen yhteys kahden identiteetillä varustetun toimijan (kuten organisaatio ja yksilö, tai yksilöt/organisaatiot keskenään) välillä on tietosuojattu eikä sitä voi korreloida toimijoiden keskenään käyttämän yhteisen virtuaalitunnisteen kanssa muihin yksilön vastaaviin sidoksiin jollei yksilö tätä erityisesti halua. Mallissa toteutuvat samanaikaisesti sekä ns. Privacy by Design että Security by Design -periaatteiden oleelliset edut joista on keskusteltu identiteetinhallinnan tutkijoiden ja asiantuntijoiden keskuudessa viimeisten vuosikymmenten aikana.

Hajautetulle, mutta luotetun ankkurin myöntämälle identiteetille voidaan myöntää virallisia varmennettavia todisteita (engl. verifiable credential) eri organisaatioiden (periaatteessa myös yksilön itsensä) toimesta. Organisaatioilla on olemassa tilikirjan kautta julkinen sähköinen identiteetti ja siihen liittyvät julkiset kuvaukset tarjotuista palveluista ja muista perustiedoista. Valtio/julkishallinto voisi myös esimerkiksi todistaa sähköisten palvelujensa (organisaatioiden) hajautettujen identiteettien aitouden allekirjoittamalla ne luottamusankkurin roolissa.



Kuva 27. Visioitu tunnus- ja lupalompakko - hajautettu suostumusten ja lupien hallintamalli julkisen tilikirjan ja lohkoketjujen avulla toteutettuna.

Identiteetin myöntämän suostumuksen olemassaolo tai identiteetille myönnetyn todistuksen voimassaolo on aina tarkistettavissa hajautetun tilikirjan kautta. Varmennetut todistukset perustuvat yhteisesti standardoitaviin skeemoihin (tietomalleihin) ja niitä allekirjoitettaminaan tarjoavien organisaatioiden luottamusverkostoon. DLT-pohjainen järjestelmä vaatii siis yhtälailla työkaluja tietojen yhteentoimivuuden ja toimijoiden luotettavuustason takaamiseksi kuin nykymuotoinen keskittämiseen ja rajapintoihin pohjautuva malli.

Julkinen tilikirjajärjestelmä ei lähtökohtaisesti koskaan talleta (tai sen ei tulisi tallettaa) yksilöivää rekisteröidyn henkilötietoa itse verkoston solmuihin. Tämän takia henkilötietojen turvallinen tallettaminen tulee tehdä tilikirjan ulkopuolella (engl. off-ledger). Käytännössä se tarkoittaa kryptografisesti suojattujen henkilötietojen tallentamista pilvipalveluissa (‘verkkoagenteissa’) tai käyttäjien omissa mobiililaitteissa.

Suostumusten antaminen ja hallinnointi rekistereineen siirtyisi käytännössä käyttäjien itse hallinnoimiin luotettuihin mobiilisovelluksiin (‘lupalompakoihin’) ja käyttäjä on vapaa avaamaan varmennettavissa olevia todistuksia tai luvitettavia Lähderekisterien rajapintoja itse luottamilleen toimijoille (kuva 23). Identiteetti ja siihen liittyvät tiedot ovat välillisesti löydettävissä tilikirjassa julkaistavan tunnistesekoitteen avulla.

Esimerkkinä, aiemmin tietojärjestelmäluvussa kuvattu suostumusrekisteri olisi aina käyttäjäkohtainen ja käyttäjä ylläpitäisi sitä vastuutettuna rekisterinpitäjänä itse omien laitteidensa kautta. Käyttäjän tietosuojan ja suostumustenhallinnan ns. single point of failure on tässä arkkitehtuurimallissa luvat, suostumusrekisterin ja yksityiset kryptografiset avaimet sisältävä sovellus ja sitä isännöivä kuluttajalaite/-laitteet. Käyttäjän yksityisten avainten hallinta on tällä hetkellä tunnustettu DLT-ehdokasteknologioiden heikko kohta - teoriassa rekisteristä voidaan rakentaa varmuuskopio jakamalla ne osiin kryptografisesti jaettuna riittävän monen luotetun lompakonomistajan kesken käyttämällä hajautettua avaintenhallinta (Distributed Public Key Infrastructure, DPKI[[20]](#footnote-19)).

Hajautettuun tilikirjaan pohjautuva suostumustenhallinnan ratkaisu pienentäisi toimiessaan huomattavasti tietosuojariskejä rekisterinpitäjien näkökulmasta, ehkä myös mahdollisia sanktiovaikutuksia jos tilikirjajärjestelmä syystä tai toisesta vikaantuisi. Hajautettujen tilikirjojen tarkka juridinen asema (voiko globaalisti hajautettu järjestelmä olla rekisterinpitäjä) tilikirjaan tallentuvien tietojen hallinnoinnin osalta yleisen TsA:n näkökulmasta on tällä hetkellä määrittämättä.

Ratkaisuilla on teknisinä ratkaisuina selkeitä etuja keskitettyihin palveluihin nähden kuten vikasietoisuus ja myönnetyn identiteetin ja tiedonsiirtojen kiistämättömyyden todentaminen tilikirjasolmujen konsensus- ja revokaatioalgoritmien avulla. Alueen teknologiat ovat vasta kilpailu- ja pilotointivaiheessa, ja toimivan käyttäjäkokemuksen rakentaminen näiden palvelujen ja keskeisen riippumattoman identiteetin ympärille on ehdottomasti myös julkishallinnolle kokeilemisen arvoinen haaste - palveluliitoskohtaiset hajautetut tunnisteet ovat kryptografisia sekoitteita kuten ‘did:sov:zhgy34hghy8yjhe3565hdgyxnm12’ ja siten vaikeasti käytettäviä interaktioissa jos ao. identiteettejä pitäisi käyttää sellaisenaan, erityisesti jos kullakin käyttäjällä on tällaisia useampia kymmeniä tai satoja. Toisaalta, kuka digitalisaation myötä kasvanut muistaa enää ihmisten puhelinnumeroita ulkoa, kun tämä ongelma on ratkaistu erilaisilla henkilökohtaisten laitteiden yhteystietosovelluksilla.

Valtiovarainministeriö on syksyllä 2017 käynnistänyt projekti henkilötunnuksen uusimisesta, Valtiokonttorin D9, VRK ja muu julkishallinto seuraavat DLT-aluetta jo mm. valtion lohkoketjuteknologiaverkoston kautta. Pilotointi konkreettisilla julkista tilikirjaa soveltavilla käyttötapauksilla olisi aloitettava ajoissa sopivissa kokeiluhankkeissa, jottei Suomen etunoja lohkoketju- ja tilikirjaratkaisuissa vesity turhaan varovaisuuteen tai hidasteluun. Hyviä käyttötapauksia piloteille löytyisi esimerkiksi D9:n ja VRK:n asiantuntijoiden luonnosteleman [Mobiililuvat-esityspaketin](https://docs.google.com/presentation/d/1REy_Aws9k4-lN0GiVF4TrIvyg8h6ffHXv8JMt2vHgDk/edit#slide=id.p) ideoista.

### Kansalaisen uusi digitaalinen tunniste

Nykyinen julkisessa hallinnossa yksilön identifioiva tunniste on henkilötunnus, jonka käyttöön tietojärjestelmissä liittyy ongelmia sekä yksilön tietosuojan että rajallisen tunnistekoodiavaruuden suhteen. Toisaalta HeTun rinnalla käytetään eri rekisteripalveluissa hajanaisesti omia sisäisiä virtuaalitunnisteita. Suomessa asuvien henkilöiden identifioimisessa käytettävä tunniste pyritään suunnittelemaan uusiksi vuosien 2018-19 aikana. Valtiovarainministeriön 21.8.2017 asettaman[[21]](#footnote-20) hanketyöryhmän tavoitteita työlle ovat mm.

* tarjota tunniste kaikille Suomeen tuleville, ei vain kansalaisille eli tarjota tunnistautumismekanismi ja sitä kautta pääsy viranomaispalveluihin myös henkilöille joilla ei ole nykyisin niihin pääsyä (esim. ei oikeutta pankkitunnuksiin)
* päästä eroon rinnakkaisista rekisteri-identiteeteistä samalle luonnolliselle henkilölle eri julkishallinnon järjestelmissä
* luoda neutraalimuotoinen tunniste joka ei kerro henkilön sukupuolta tai syntymäaikaa
* pystyä hallinnoimaan tunnusta ja siihen liittyviä attribuutteja erillisinä prosesseina
* edistää rekisteritietojen hajautettua hallintaa
* soveltaa *tietoa kysytään vain kerran* -periaatetta tunnisteen käytössä eri rekisteripalveluissa
* mahdollistaa tunnuksen avulla siihen liitettyjen yksilön omien tietojen hallinta ja hyödyntäminen sekä julkisella että yksityisellä sektorilla
* identiteettivarkauksien estäminen

Tunnisteen suunnittelussa otetaan huomioon myös kansainvälinen kehitystilanne ja erilaiset yhteensopivuusvaatimukset tunnistautumismekanismien (esimerkiksi eIDAS) ja yksilön henkilöllisyyden tunnistamisen vahvuustason osalta (kuten NIST:in em. muutos määrittelyjen osalta).

Hajautettu riippumaton identiteetti (ks. yllä) on myös yksi mahdollinen ja julkishallinnon näkökulmasta mielenkiintoinen ratkaisumalli. Tosin asetettuja tavoitteita vasten sen toteutus tulisi eteen todennäköisesti rajoitetulla mallilla, jossa yksi hajautettu identiteetti olisi käytössä kaikissa julkishallinnon palveluissa - siis tapana poistaa nykyinen sekava käytäntö eri hallinnonalojen virtuaalitunnisteiden käytössä.

Tavoitteista ilmi käyvä ns. selektiivinen attribuuttien julkaiseminen (engl. selective disclosure) ja ‘epäsuora’ attribuuttipohjainen tunnistaminen tai henkilöön liittyvien tietojen verifiointi on mahdollista toteuttaa useilla tunnistautumisarkkitehtuurin toteutustavoilla (sekä keskitetysti että hajautetusti).

Uuden tunnisteen suunnittelun vaikutukset suostumustenhallinnan ratkaisemisessa ovat merkittäviä, siksi työryhmän kanssa tulee keskustella säännöllisesti uudistamistyön edetessä ehdotusten tasolle.

# Liitteet

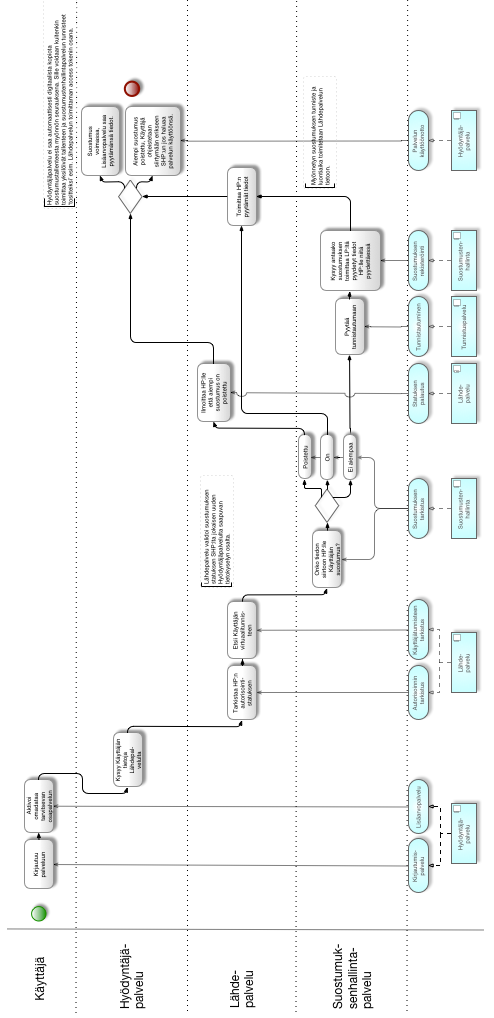
Liite 1 - luonnosteltuja OPH:n, Veron, Helsingin kaupungin ja Trafin omadata-käyttötapauksia

[Liite 2](#_aaj1jntiiotb) - Suostumuskysely prosessikaavio

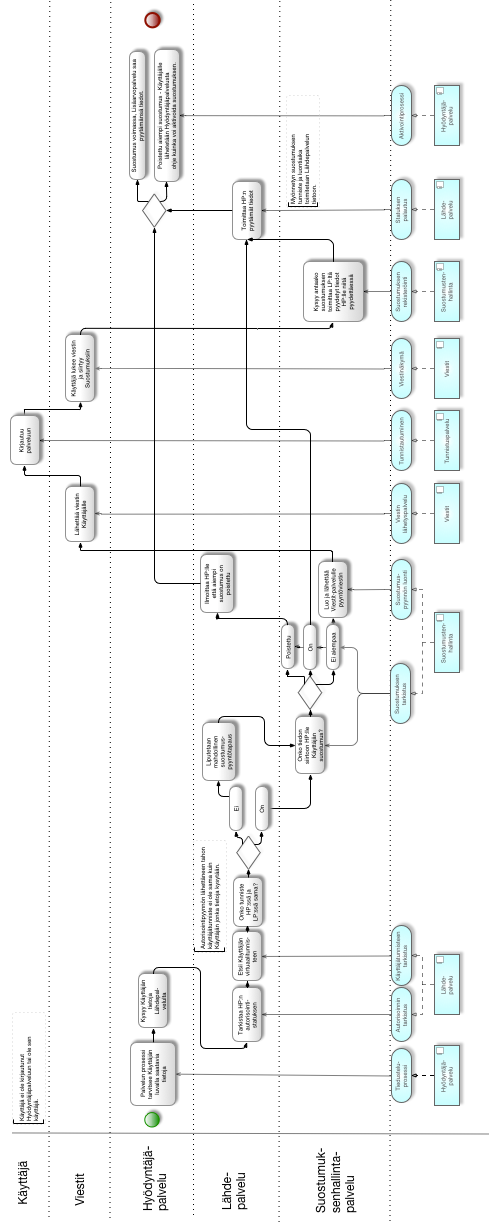
[Liite 3](#_47cl6nfjci8v) - Suostumuspyyntö prosessikaavio

Liite 1 (pp-esitys)

## Liite 2 - Suostumuskyselyn prosessikaavio ([PDF originaali](https://drive.google.com/file/d/1BwDxKDPMHCO72O9eicpozrqCfqXgflVV/view?usp=sharing))



## Liite 3 - Suostumuspyynnön prosessikaavio ([PDF originaali](https://drive.google.com/file/d/1HpC4SmF_WmkPxJghs9xU9w8n0ffDJxqr/view?usp=sharing))



1. <https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource> [↑](#footnote-ref-0)
2. <http://vm.fi/yhteinen-tiedon-hallinta> (2016-2018) [↑](#footnote-ref-1)
3. Tietotekniikan termitalkoot 2016-11-11: [www.tsk.fi/tsk/termitalkoot/fi/node/266](http://www.tsk.fi/tsk/termitalkoot/fi/node/266) [↑](#footnote-ref-2)
4. Suostumuksen ja valtuutuksen eroista <http://oulu.ouka.fi/kehittamishankkeet/kehittamishankkeet2000alkaen/hankkeet/loppuraportit/Suostumus%20ja%20Valtuutus%20m%C3%A4%C3%A4rittelyt.pdf> [↑](#footnote-ref-3)
5. [Palveluhallinnan yleisesittely](https://palveluhallinta.suomi.fi/fi/sivut/palveluhallinnasta/yleisesittely) [↑](#footnote-ref-4)
6. Palvelutietovarannon esittely ks. <https://esuomi.fi/palveluntarjoajille/palvelutietovaranto/> [↑](#footnote-ref-5)
7. Palveluväylään liittyvät käsitteet (Palveluväylä, Liityntäpalvelin, X-Road) määritelty <https://esuomi.fi/palveluntarjoajille/palveluvayla/sanasto/> [↑](#footnote-ref-6)
8. MyData muutosvoimana: Julkishallinnon henkilötiedon ihmiskeskeisen hyödyntämisen mallit ja vaikutukset. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 61/2017 [↑](#footnote-ref-7)
9. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80098/OMML\_35\_2017\_EUn\_yleinen\_tietosuoja.pdf?sequence=1 [↑](#footnote-ref-8)
10. MyData muutosvoimana: Julkishallinnon henkilötiedon ihmiskeskeisen hyödyntämisen mallit ja vaikutukset, <http://tietokayttoon.fi/julkaisu?pubid=21301> [↑](#footnote-ref-9)
11. <http://vm.fi/digitalisoinnin-periaatteet> [↑](#footnote-ref-10)
12. Lisätietoja: https://fi.okfn.org/?s=s%C3%A4hk%C3%B6inen+asiointi+ja+henkil%C3%B6tieto [↑](#footnote-ref-11)
13. .well\_known URI:en käytöstä ks. kappale 5 dokumentissa [MyData Architecture Framework 2.0](https://github.com/mydata-sdk/mydata-docs/blob/master/architecture_specs/MyData%20Architecture%20Framework%202.0.pdf)  [↑](#footnote-ref-12)
14. Ks. Kelan englanninkielinen [autorisointiopas](http://www.kanta.fi/documents/12105/4106842/PHR+authorization/b2135f9f-5bfb-49d8-827e-4f5b44cdab2e) PHR-sovellusten kehittäjille [↑](#footnote-ref-13)
15. http://ec.europa.eu/newsroom/just/document.cfm?doc\_id=48849 [↑](#footnote-ref-14)
16. Suostumustallenteiden toteuttamisesta tarkemmin ks. esim. [MyData Consenting Specification](https://github.com/mydata-sdk/mydata-docs/blob/master/architecture_specs/MyData%20Architecture%20Framework%20-%20Consenting%20Specification.pdf) [↑](#footnote-ref-15)
17. Suostumustallenteiden toteuttamisesta tarkemmin ks. esim. [MyData Consenting Specification](https://github.com/mydata-sdk/mydata-docs/blob/master/architecture_specs/MyData%20Architecture%20Framework%20-%20Consenting%20Specification.pdf) [↑](#footnote-ref-16)
18. [MyData Architecture Framework - Service Linking](https://github.com/mydata-sdk/mydata-docs/raw/master/architecture_specs/MyData%20Architecture%20Framework%20-%20Service%20Linking%20Specification.pdf) [↑](#footnote-ref-17)
19. [Palveluväylän viitearkkitehtuuri 2.0 - Liite 3 Rajapinnan kuvaus](https://www.avoindata.fi/data/fi/dataset/kansallisen-palveluvaylan-viitearkkitehtuuri/resource/a134bfe8-b1cf-405e-8f39-cae1a06c1802?inner_span=True) [↑](#footnote-ref-18)
20. https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust/blob/master/final-documents/dpki.pdf [↑](#footnote-ref-19)
21. http://valtioneuvosto.fi/hanke?tunnus=VM068:00/2017 [↑](#footnote-ref-20)