Juha Mykkänen, Hannu Virkanen, Saara Savolainen

# Vaatimukset ja rajaukset palvelupohjaiselle käyttäjä- ja käytönhallinnalle

SOLEA-hanke
Itä-Suomen yliopisto
Aalto-yliopisto

ITÄ-SUOMEN YLIOPISTO

Aalto-yliopisto
Teknillinen korkeakoulu

Juha Mykkänen, Hannu Virkanen, Saara Savolainen

# Vaatimukset ja rajaukset palvelupohjaiselle käyttäjä- ja käytönhallinnalle

Itä-Suomen yliopisto ja Aalto-yliopisto
Kuopio
2012

ITÄ-SUOMEN YLIOPISTO

Aalto-yliopisto
Teknillinen korkeakoulu

©Itä-Suomen yliopisto ja Aalto-yliopisto 2012
SOLEA-hanke
http://www.uef.fi/solea

ISBN 978-952-61-0726-4 (PDF)

Juha Mykkänen, Hannu Virkanen, Saara Savolainen. Vaatimukset ja rajaukset palvelupohjaiselle käyttäjä- ja käytönhallinnalle. Itä-Suomen yliopisto ja Aalto-yliopisto. 2012. 63 s.
ISBN 978-952-61-0726-4 (PDF)

## Tiivistelmä

Käyttäjä- ja käytönhallinta on organisaation tietohallinnon ja tietojärjestelmien osa-alue, joka muodostaa keskeisen osan tietotekniikkatoimintaa. Alue on sangen haasteellinen, koska yleensä se koskettaa kaikkia tietotekniikan kanssa toimivia työntekijöitä ja usein myös kaikkia asiakkaita. Samaten organisaatioissa voi olla suuri joukko eri ikäisiä ja eri lähteistä peräisin olevia tietojärjestelmiä, joiden käyttäjä- ja käytönhallinnan yhteensovittaminen on haastava tehtävä. Organisaatioiden verkostomainen yhteistoiminta asettaa tätäkin suurempia haasteita käyttäjä- ja käytönhallinnan toimivalle järjestämiselle.

SOLEA-hanke (2008-2012) on tutkinut ja kehittänyt palveluarkkitehtuurin soveltamista osana organisaatioiden kokonaisarkkitehtuuria. Hankkeen lähestymistapana oli tutkia, kehittää ja soveltaa palvelukeskeisiä ja kokonaisarkkitehtuuriin liittyviä menetelmiä ja malleja liittyen osapuolten omiin kehittämistarpeisiin. Keskeinen osa tätä oli organisaatioiden omien tai yhteisten kehittämiskohteiden tukeminen tiettyyn kohdealueeseen kohdistuvan case-työn kautta. Käyttäjä- ja käytönhallinta oli yksi tällainen useiden organisaatioiden esiin nostama kehittämisalue.

Tässä dokumentissa kootaan SOLEA-hankkeen käyttäjä- ja käytönhallinta -työkohteen tuloksia. Dokumentissa kuvataan käyttäjä- ja käytönhallinnan keskeisiä käsitteitä sekä eri tahoilla tunnistettuja käyttäjä- ja käytönhallinnan kehittämistarpeita. Käyttäjähallinta-kohdealueelle esitetään jäsentämismalli sekä perusprosessit ja toiminnot, joita voidaan tunnistaa ja hyödyntää eri organisaatioissa ja hankkeissa kehitettävien käyttäjä- ja käytönhallinnan ratkaisujen pohjana. Keskeisiä käyttäjä- ja käytönhallintaan liittyviä suunnittelupäätöksiä käsitellään eri suunnitteluvaihtoehtoineen. Aihealueen tukemiseen tietojärjestelmissä esitetään palvelupohjainen jäsennys, jossa on tunnistettu joukko eri tavoin toteutettavissa tai hankittavissa olevia tietojärjestelmäpalveluja. Keskeisimmistä tietojärjestelmäpalveluista esitetään tarkemmat kuvaukset. Lisäksi kartoitetaan lyhyesti joukko valmiita malleja ja teknisiä standardeja käyttäjä- ja käytönhallinnan eri aspektien toteuttamiseksi ja yhteensovittamiseksi.

Edellä kuvatun jäsennys- ja valmiiden mallien kokoelman lisäksi dokumentin liitteessä käydään läpi case-esimerkki kuvattujen mallien käytöstä sairaanhoitopiirin kehittämishankkeiden suunnittelussa. Case-esimerkistä kuvataan toteutustapa, hyödynnetyt mallit sekä esimerkkejä tuloksista. Esimerkin osalta kuvataan myös aiheeseen liittyvästä toisesta osatutkimuksesta hyödynnettyjen kuvausten tiedonkeruupohjien hyödyntäminen. Menetelmien ja jäsennysten hyödynnettävyyttä on arvioitu case-esimerkin osallistujien toimesta. Mallien käyttämisen ja työpajamaisen läpikäynnin todettiin edesauttavan tarkempien projektien suunnittelua ja ongelmakentän jäsentämistä.

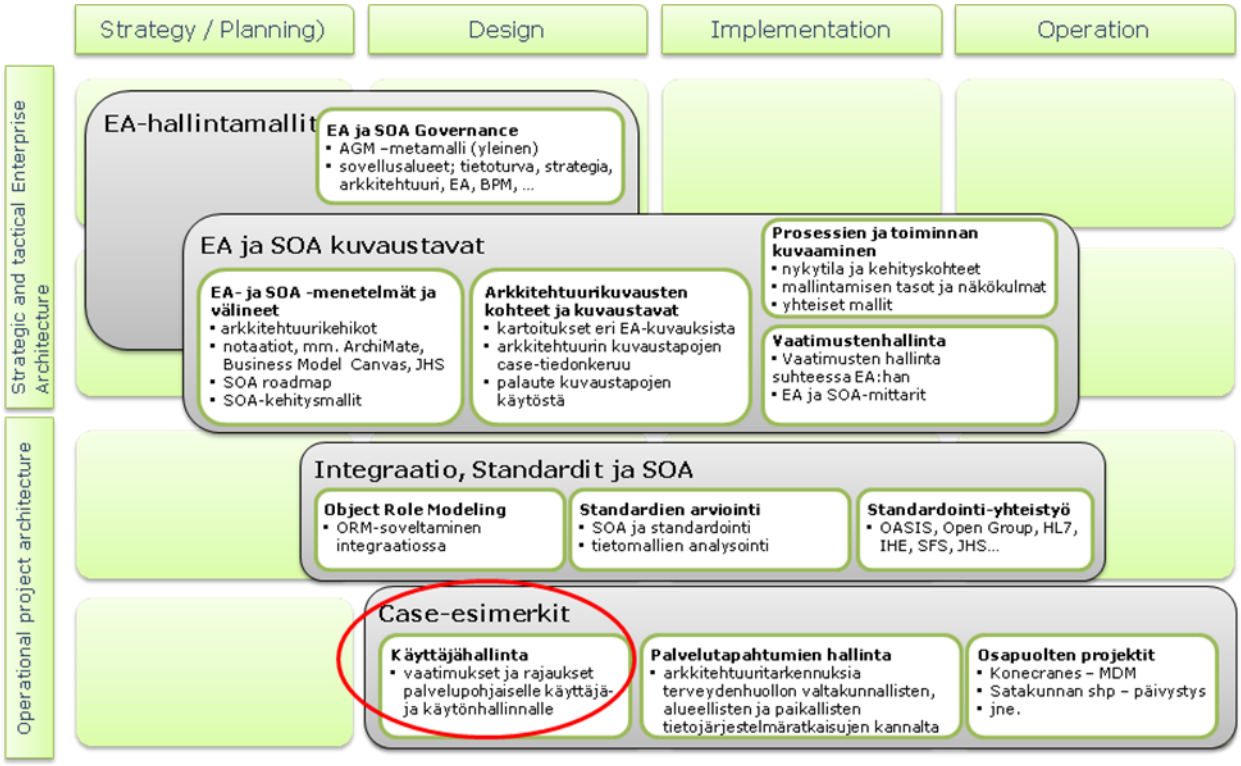
Luokitus (UDK): tietotekniikka 004, internet 654 & 004, tietojenkäsittely 004

Asiasanat (YSA): tiedonhallintajärjestelmät, verkkopalvelut, järjestelmäarkkitehtuuri, ohjelmistokehitys, standardit, ohjelmistotuotanto, prosessit, hajautetut järjestelmät, systeemityö, protokollat

## Sisällys

# 1 Johdanto

SOLEA-hankkeessa on tutkittu ja kehitetty palvelukeskeisen arkkitehtuurin (SOA)hyödyntämistä osana organisaatioiden kokonaisarkkitehtuuria (EA) vuosina 2008-2011. Hankkeen tutkimustulosten ja menetelmien avulla tehostetaan kokonaisarkkitehtuurin kehittämistä ja hallintaa sekä yksittäisten organisaatioiden että toimialakohtaisten kohdealueiden osalta, ja tuetaan projektien toimintaa ja hallittavuutta.




**Kuva 1:** Tämän dokumentaation osa-alue SOLEA-hankkeen kokonaisuudessa.

Käyttäjähallinta -kohteen työ liittyy SOLEA-hankkeeseen (palvelupohjainen paikallisesti sovitettava kokonaisarkkitehtuuri). SOLEA- hankkeessa tutkitaan ja kehitetään palveluarkkitehtuurin (SOA) hyödyntämistä osana organisaatioiden kokonaisarkkitehtuuria (EA). Tavoitteena on tutkia, kehittää ja mitata palvelupohjaisen kehitystavan hyötyjen (joustavuus ja liitettävyys) saavuttamista. Kehittämistyössä tavoitteena on, että liiketoiminnan / toiminnan kehittämisen ja teknisen kehityksen välimatka pienenee, ja että kokonaisjärjestelmän kehityssyklit nopeutuvat. Hankkeessa keskitytään osapuolten kannalta olennaisimpiin arkkitehtuuri- ja integraationäkökulmiin, joita voidaan soveltaa osapuolten toiminnassa. Hanketta rahoittavat Tekes (päätös nro 40127/08) sekä joukko yrityksiä ja sairaanhoitopiirejä.

Tämä dokumentti kokoaa SOLEA-hankkeen Käyttäjähallinta -kohteen työn tuloksia. Työssä sovelletaan useita palveluarkkitehtuurin ja kokonaisarkkitehtuurin sekä käyttäjähallinnan erityisalueen valmiita menetelmiä ja malleja (joita ei kuitenkaan käsitellä laajemmin tässä dokumentissa).[1]

[1] Normalisoitu EA-malli, RM-ODP, palveluarkkitehtuuriin sovellettu EA grid, SOMA-viitearkkitehtuuri, prosessisn ja toiminnan mallinnuksen 6-tasomalli, 4-tasoinen governace-malli

Ensimmäisenä tavoitteena on jäsentää Käyttäjähallinta-kohdealue kokonais- ja palveluarkkitehtuurilähestymistavalla siten että sieltä on tunnistettavissa hankeen osapuolten yhteisesti tai omassa toiminnassa hyödynnettävissä ja työstettävissä olevia tarkempia kohteita. Toisena tavoitteena on tarkentaa, millaisia yhteisiä ratkaisuja ja malleja ko. alueeseen liittyen etsitään tai määritellään hankkeen puitteissa. Tavoitteena on täydentää osapuolten omassa toiminnassa tehtävää työtä ja keskittyä yhteisesti ratkaistaviin tai tarkennettaviin seikkoihin.

# 2 Keskeisiä käsitteitä

Käyttäjähallintatyön osalta pyritään soveltamaan mahdollisimman sellaisenaan VAHTI-sanastoa (VAHTI 2006). Keskeisimpiä käytettäviä käsitteitä ovat:

| | | |
|---|---|---|
| identiteetti | Identity | joukko ominaisuuksia, jotka kuvaavat käyttäjää ja joiden avulla käyttäjä voidaan tunnistaa |
| identiteettien yhdistäminen/ federointi | identity federation | käyttäjän erillisten käyttäjäidentiteettien kytkeminen toisiinsa |
| käyttäjä | user; principal (Liberty Alliance) | tietojärjestelmäpalveluja käyttävä henkilö, ryhmä tai ohjelmisto |
| käyttäjähallinta | user management; identity management | käyttäjäidentiteetti- ja käyttäjätilitietojen ylläpito |
| käyttäjäprofiili | user profile | palvelujärjestelmässä ylläpidettävät käyttäjätiliin liittyvät ominaisuudet, mm. käyttäjärooli; Käyttäjäprofiilin avulla voidaan ohjata palvelujen käyttöä |
| Käyttäjärooli | user role | joukko käyttäjän ominaisuuksia, jotka liittyvät hänen tietotarpeittensa ja/tai toimintavaltuuksiensa määrittelyyn; Käyttäjäroolia voidaan katsoa joko käyttäjän toimenkuvan näkökulmasta (työrooli) tai hänellä palvelujärjestelmissä olevien valtuuksien näkökulmasta |
| Käyttäjätili | user account | käyttäjän ja palveluntarjoajan välinen sopimus, joka mahdollistaa verkkopalvelujen käytön |
| Käyttäjätunnus | user name, user identifier, user ID | tunnistamista varten annettu käyttäjätilin yksilöivä tunniste |
| käyttövaltuus; käyttöoikeus | usage right; access right | tietojärjestelmän käyttäjälle tai esimerkiksi tietyn käyttäjäroolin omaavalle käyttäjäryhmälle myönnetty yksilöity oikeus nimetyn palveluelementin tai muun kohteen käyttöön; Käyttövaltuus määrittelee, miten ja millaisilla edellytyksillä käyttäjällä on oikeus käyttää ao. palveluelementtiä |
| Luottamusverkosto | circle of trust, trust circle, federation | joukko palvelutarjoajia ja tunnistajia, joiden kanssa käyttäjät voivat asioida turvallisesti kuin yhdessä ympäristössä |
| provisiointi | Provisioning | käyttäjä- ja käyttövaltuustietojen välittäminen palvelujärjestelmiin |
| pääsynvalvonta | access control | tiedot, toiminnot ja menettelyt, joiden avulla palvelujärjestelmän tai sen palveluelementtien käyttö mahdollistetaan vain valtuutetuille käyttäjille |

| | | |
|---|---|---|
| pääsynvalvontapiste | Policy Enforcement Point | palvelu, joka "vartioi" suojattua resurssia tai palvelua tarkastamalla tehtyjä pyyntöjä ja myöntää tai estää pääsyn |
| todennus; todentaminen | authentication; verification | käyttäjän aitoudesta varmistuminen halutulla luottamustasolla; Todentamisessa nojaudutaan johonkin jota a) käyttäjä tietää, b) käyttäjällä on tai c) käyttäjä on |
| tunnistaja; tunnistuspalvelu | Authenticator | verkkopalvelun komponentti tai osapuoli, joka huolehtii käyttäjien tunnistamisesta ja todentamisesta |
| tunnistautuminen | Identification | menettely, jossa käyttäjä esittää tunnistetietonsa |
| tunnistus; tunnistaminen | Identification | menettely, jolla yksilöidään joku tai jokin, esimerkiksi tietojärjestelmän käyttäjä; Sähköiseen tunnistamiseen liittyy normaalisti aina myös käyttäjän todentaminen. Tunnistaminen voi perustua **tunnistautumiseen** tai olla passiivista tunnistamista, joka ei edellytä tunnistettavalta toimintaa ja jossa tunnistettava ei välttämättä tiedä tulevansa tunnistetuksi |
| tunnistusseloste; seloste | Assertion | tunnistajan palvelujärjestelmälle toimittama selvitys, joka sisältää todennettua käyttäjäidentiteettiä vastaavia tietoja ao. käyttäjästä; Esimerkkejä tunnistusselosteista ovat SAML-selosteet ja evästeet |
| Työrooli | business role | käyttäjän toimenkuvaan kuuluvat tietotarpeet ja toimintavaltuudet |
| vahva tunnistus; vahva tunnistaminen | strong identification | käyttäjän tunnistaminen käyttäen vähintään kahta eri todennustapaa |
| valtuutus | authorisation; authorization | todennetulle käyttäjälle annettu lupa tietyn tiedon, suojattavan kohteen tai muun palveluelementin käyttöön voimassa olevien pääsynvalvontatietojen perusteella |
| verkostoidentiteetti; yhdistetty identiteetti | network identity, federated identity | käyttäjän yhdistettyjen käyttäjäidentiteettien yhdessä määrittelemä joukko käyttäjän ominaisuuksia |

# 3 Käyttäjähallinta - yhteisiä kehittämistarpeita

Käyttäjähallinta (myös käyttäjä- ja käytönhallinta, Identity Management IdM, Identity and Access Management IAM) on keskeinen osa tietojärjestelmäkokonaisuuksien käyttöä ja hallintaa. Se on nähtävissä keskeisenä osana organisaatioiden tietojärjestelmäinfrastruktuurissa. Käyttäjähallinta yhdistyy lukuisiin eri sovelluksiin, prosesseihin ja teknisiin ratkaisuihin monimutkaisissa tietojärjestelmäympäristöissä. Monet käyttäjähallinnan osaratkaisuista voidaan nähdä yli toimialarajojen hyödynnettävinä ydinpalveluina. Palveluarkkitehtuurin ja kokonaisarkkitehtuurin kannalta käyttäjähallinta on yksi tärkeimpiä tukipalveluita tai infrastruktuurialueita, josta suuri joukko muita palveluja on riippuvaisia, ja jonka yhtenäistäminen esim. eri sovellusten välillä poistaisi runsaasti ylimääräistä ylläpito- ja hallintatyötä. Käyttäjähallintaan liittyvien palvelujen on nähty myös tarpeelliseksi olla käytettävissä yli organisaatiorajojen. SOLEA-kohdistuskyselyssä ja kokouksissa on osapuolilla todettu olevan jo käytössä uudelleenkäytettävänä yleispalveluna mm. käyttöoikeuksien hallintaan

liittyviä palveluja, ja esimerkiksi asiakkaan tunnistuksen osalta on nähty useita mahdollisia yhteisiä kehittämiskohteita.

3.11.2008 järjestetyssä työkokouksessa tarkennettiin tarpeita ja toimenpiteitä SOLEA-käyttäjähallintatyöhön liittyen. Lisäksi hankkeen kohdistuskyselyssä, osapuolitapaamisissa, työpajaseminaarissa sekä osapuolten materiaalissa ja tapahtumissa (mm. 18.11.2008) on tunnistettu monia tarpeita ja vaatimuksia käyttäjähallinnan kehittämiseen.

Tarpeiden prioriteetit vaihtelevat organisaatio- tai hankekohtaisesti. Keskeisiin tarpeisiin ja vaatimuksiin on tunnistettu mittareita[2], joilla voidaan seurata niiden toteutumista. Tarkennettua yleistä vaatimuslistaa ei esitetä tässä yhteydessä, vaan vaatimuksia tarkennetaan osa-alue- ja palvelumäärittelykohtaisesti.

| **Kehittämistarve** | **Mittarit** |
|---|---|
| Käyttäjähallinnan yhdistäminen henkilöstöhallinnon prosesseihin. | Henkilöstöhallinnon lisäksi muualla tarvittavien käyttäjähallinnan toimenpiteiden työmäärä.<br>Erillisten käyttäjähallintaan liittyvien (henkilöille kohdistuvien) palvelupyyntöjen määrä. |
| Käyttäjien tunnistaminen ja todentaminen yhdenmukaisesti. | Erilaisten tunnistamis- ja todentamistapojen lukumäärän väheneminen<br>Yhdenmukaisten tunnistamis- ja todentamispalvelujen käyttöaste (kuinka suuri osuus sovelluksista tai tunnistustapahtumista käyttää yhdenmukaisia palveluja) |
| Käytäntöjen yhtenäistäminen eri sovelluksissa liittyen käyttäjien ja käytön hallintaan | Yhtenäisiä käyttäjähallinta-, tunnistus- ja pääsynvalvontaratkaisuja käyttävien sovellusten tai käyttötilanteiden osuus kaikista. Yhden käyttäjän käyttäjätilien lukumäärä. Ylläpitotyön määrä ja kustannukset käyttäjätunnusten tekoon. Käyttövaltuuksien saannin ja käsittelyn odottamiseen kuluva aika. |
| Käyttäjätietojen yhdistäminen henkilöiden työrooleihin ja staattisiin käyttöoikeuksiin | Käyttöoikeuksien määrittelyt on sidottu rooleihin. Käyttäjien määrittely voidaan tehdä erillään työroolien määrittelyistä. (RBAC, role-based access control). |
| Käyttäjähallinnan yhdistäminen dynaamisiin, vuorovaikutussuhteista tai muista henkilöistä riippuviin käyttöoikeuksiin (esim. asiayhteyden päättely terveydenhuollossa) | Tarkastus: voidaanko käyttövaltuuksien tarkastamisen yhteydessä huomioida tarvittavia dynaamisia vuorovaikutussuhteita. |
| Kertakirjautuminen (SSO) | Käyttäjän kirjautumistoimenpiteiden lukumäärä / ajanjakso. Käyttäjän käyttäjätunnusten tai käyttäjätunnus / salasanaparien lukumäärä. Kirjautumistoimenpiteisiin käytetty aika / ajanjakso. Kirjautumistransaktion hinta. |

[2] Mitattavia seikkoja: käyttäjä / asiakastyytyväisyys-mittarit, käytettävyys / saatavuus, toimintaprosessien mittarit, tietojen mittarit, kehitysprosessin mittarit, tekniset mittarit
Mittareiden tyyppejä: lukumäärä, työmäärä / ajallinen, laadullinen, taloudellinen
[Palveluarkkitehtuurin soveltaminen terveydenhuollossa, osa 1, luku 4.3.]

| | |
|---|---|
| Vahvan tunnistamisen käyttöönotto, ulkoisten varmennepalvelujen tai toimikorttien käyttöönotto | Ratkaisujen kautta hoidettava osuus tunnistustapahtumista. Ko. ratkaisuilla hoidettavien tunnistamistapahtumien lukumäärä. Ratkaisujen piirissä olevien sovellusten lukumäärä ja osuus kaikista sovelluksista. |
| Organisaation ulkopuolisten käyttäjien huomiointi käyttäjähallintaratkaisuissa. | Esimerkiksi federoidun käyttäjähallintaratkaisun (ml. toimintatavat) käyttöönoton onnistuminen. Ks. myös edellinen rivi. |

Yleisiksi ja useita osapuolia palveleviksi toimenpiteiksi käyttäjähallinnan osalta on tunnistettu seuraavia:

- yhteisten käsitteiden kartoitus ja valinta
- SOA-palvelujen tunnistaminen käyttäjä- ja pääsynhallintaan
- eri palveluista koostuvien sovellusten ja prosessien yhdenmukaisten käyttäjähallintaratkaisujen etsiminen tai kehittäminen
- käyttäjähallinnan järjestelmällisen jäsentämismallin valinta tai kehittäminen
- federoidun käyttäjähallinnan käyttömahdollisuuksien ja -tilanteiden tarkentaminen
- käyttäjähallinnan työnjaon tarkentaminen suhteessa toiminnassa käytettäviin ydin- tai toiminnanohjausjärjestelmiin ja kaupallisiin IdM/IAM-tuotteisiin
- uusilta järjestelmiltä vaadittavan yhteisen rajapinnan määrittely siten, että voidaan huomioida myös pienet uudet sovellukset ja toimittajat

**Erityiskysymyksiä ja lisähuomioita tarpeisiin:**

Yksiköstä toiseen siirtyvien käyttäjien hallinta
Käyttäjän sujuva vaihtaminen työasemilla, jotka ovat yhteiskäytössä
Käyttäjähallinnan toteuttavien palvelujen palvelutaso (saatavuus, maksimituntimäärä poissa käytöstä, vasteajat, suorituskyky)
Poistettujen käyttäjien tiedot voitava edelleen jäljittää, esim. muutoksmerkinnöistä ja lokeista.

# 4 Käyttäjähallinnan jäsentämismalli

Keskeisenä on nähty eri tyyppisten "käyttäjätyyppien" ja kentän "päätoimintojen" mukainen luokittelu, jonka mukaisesti tarpeita ja ratkaisuja jäsennetään.

| | organisaation hallinnoimat käyttäjät / työntekijät | asiakas- tai kansalaiskäyttäjät | kumppaniorganisaatioiden hallinnoimat käyttäjät (luottamusverkosto) |
|---|---|---|---|
| käyttäjien, roolien ja valtuuksien määrittely | | | |
| käyttäjien tunnistaminen ja todentaminen | | | |
| pääsynvalvonta | | | |
| käytön seuranta | | | |

Taulukon riveillä on keskeisimmät toiminta-alueet, joille käyttäjähallintatyötä kohdistetaan ensi vaiheessa. Käytön seurantaa ei pidetty olennaisimpana tarkennusta vaativana osa-alueena (esim. lokiratkaisuja on olemassa).

Kussakin taulukon kentässä voidaan tarkastella tarvittavia käytäntöjä, prosesseja tai toimintoja, teknologioita, erilaisten luottamus/vahvuus tavoitetasojen sekä keskittämisen tavoitetasojen tunnistamista, tietojen kopiointia tai provisiointia, master data-määrittelyjä ja muita tarvittavia seikkoja. Useita keskeisistä suunnittelupäätöksistä käsitellään luvussa 6. Eri kenttiin saadaan osin yhteisiä, osin erillisiä ratkaisuja.

# 5 Käyttäjähallinnan perusprosessit ja toiminnot

Käyttäjähallinnan palvelupohjaiseen tarkentamiseen on sovittu käytettäväksi ensisijaisesti toiminta- ja prosessilähtöistä (top-down) jäsentämistapaa. Tässä luvussa kuvataan käyttäjä- ja käytönhallinnan keskeiset prosessit, toiminnot, tehtävät ja teot, jotka liittyvät sovellusten käytön yhteydessä tarvittaviin käyttäjien ja järjestelmien tai sovelluspalvelujen toimenpiteisiin tai toimintoihin. Toiminnallista jäsentämistä voidaan tehdä konteksti-, yleiskuva-, prosessi-, toiminto-, tehtävät- ja teko/operaatio -tasoilla. Tässä luvussa viitattavat ”tasot” seuraavat SOLEA-hankkeen kuusitasoista toiminnan ja prosessien kuvaamisen jäsennystä (Luukkonen ym. 2012).

Käyttäjähallinnassa ei ole vain yhtä perusprosessia, vaan se liittyy eri osa-alueilla erilaisiin prosesseihin ja etenkin tietojärjestelmien käyttöön ja ylläpitoon.

Käytännön tehtävät ja ratkaisut kussakin prosessissa ja toiminnossa voidaan tarkentaa keskeisten kohderyhmätyyppien (organisaation työntekijä, asiakas tai kansalainen, luottamusverkosto) mukaisesti. Samoja ratkaisuja voidaan joissakin tilanteissa käyttää eri kohderyhmille. Tehtävät ja teot on erotettu tarvittavista välineistä tai tietovarastoista.

**1 Käyttäjien ja roolien määrittely**

Henkilöstöhallinnon asiaan liittyvät pääprosessit (prosessitaso):

1.1. työntekijän työsuhteen aloittaminen
1.2. työntekijän aseman muuttaminen (yksikön vaihto, ylennys, projekti tms.)
1.3. työntekijän työsuhteen päättäminen

Käyttäjähallinnon työnkulut (aliprosessit –taso (työnkulut)):

1.4. käyttövaltuuksien hakeminen
1.5. käyttövaltuuksien puoltaminen ja hyväksyminen
1.6. käyttövaltuuksien poisto
1.7. edustajuuden (toisen puolesta toimiminen) ylläpito
1.8. unohtuneen salasanan palauttaminen tai uusiminen

Edellä kuvattuihin prosesseihin ja työnkulkuihin liitetään usein automatisointitavoitteita käyttäjähallinnan tehostamiseksi. Vastaavia työnkulkuja kuin käyttövaltuuksiin liittyvät voidaan tunnistaa myös esimerkiksi toimikortteihin liittyen (hakeminen, hyväksyminen, poisto jne.).

Käyttäjähallinnan toimenpiteitä, joihin voidaan kohdistaa automatisointitavoitteita esim. suhteessa henkilöstöhallinnon prosesseihin (tehtävätaso):

1.9. käyttäjätilin lisääminen
1.10. käyttäjän valtuuksien määrittely / liittäminen järjestelmärooleihin
1.11. käyttäjätilin poistaminen tai disablointi
1.12. työ- ja järjestelmäroolien ylläpito (määrittely, lisääminen, valtuuksien määrittely, poistaminen)
1.13. käyttäjätietojen provisiointi esim. keskitetystä käyttäjähallintavarastosta
1.14. salasanan vanhentuminen
1.15. salasanan vaihtaminen
1.16. yhdistetyn käyttäjäidentiteetin ylläpito

## 2. Käyttäjien tunnistaminen ja todentaminen (tehtävä- ja teko -tasot)

2.1. tunnistautuminen, sisältäen tunnistetietojen esittämisen, tunnistamisen ja todentamisen
2.2. käyttäjän todentaminen, ilman tunnistetietojen erillistä esittämistä
2.3. sisäänkirjautuminen järjestelmään (automatisoitu esim. kertakirjautumisen yhteydessä, tai tunnistautumisen sisältävä)
2.4. uloskirjautuminen järjestelmästä
2.5. käyttäjän vaihto (sisältäen uloskirjautumisen ja sisäänkirjautumisen)
2.6. sähköinen allekirjoitus (voi hyödyntää samaa tunnistamis/todentamisinfrastruktuuria)

Tunnistamistarpeen ja todentamisen vahvuuden määrittely on tehtävä käyttäjäryhmittäin ja käyttötilannekohtaisesti. Myös resurssien anonyymikäyttö on mahdollista.

## 3. Pääsynvalvonta

Käyttäjän käyttövaltuuksien tarkistaminen (käyttötilanteita mm.: resurssin käytön yhteydessä, sisäänkirjautumisen jälkeen tai yhteydessä, käyttäjän vaihtumisen yhteydessä), voi sisältää esim. seuraavia operaatioita / tekoja:

3.1. käyttäjäidentiteetin todentaminen käyttövaltuustarkistuksen yhteydessä
3.2. käyttäjäprofiilin perusteella tehtävä käyttövaltuustarkastus
3.3. käyttäjäprofiiliin kuuluvien roolitietojen (työrooli, järjestelmärooli) perusteella tehtävä käyttövaltuustarkastus
3.4. käyttökontekstitietojen (esim. sijainti, aika, asiakassuhde, suostumus) perusteella tehtävä käyttövaltuustarkastus
3.5. käyttäjän session voimassaolon tarkastaminen (mikäli tehdään sessionhallintaan liittyen)
3.6. resurssin käyttöön liittyvän käyttöpolitiikkamäärityksen (policy) noutaminen ja evaluointi suhteessa käyttäjäprofiili- ja käyttökontekstitietoihin

sekä:

3.7. resurssien käyttöön tarvittavien käyttäjä-, rooli- ja kontekstitietojen määrittely ja ylläpito (tehtävät)
3.8. lokien päivitys (tehtävä)
3.9. käytön raportointi (tehtävä)

# 6 Käyttäjähallinnan keskeisiä suunnittelupäätöksiä

Käyttäjä- ja pääsynhallinnan arkkitehtuurin määrittelemiseksi on tehtävä joukko keskeisiä suunnittelupäätöksiä. Tässä luvussa esitetään etenkin sovellus- ja arkkitehtuurinäkökulmasta tähän liittyviä keskeisiä suunnittelupäätöksiä. Keskeisimmät päätökset ovat:

- mitkä toiminnot, työnkulut tai prosessit pyritään yhdenmukaistamaan tai automatisoimaan?
- mitkä palvelut ja järjestelmät otetaan keskitetyn käyttäjä- ja valtuushallinnan tai kertakirjautumisen piiriin?
- missä määrin eri käyttäjäryhmiä ja myös käyttäjien ja sovellusten pääsynhallintaa pyritään kehittämään samoilla ratkaisuilla?
- millaisia turvatasoja määritellään (huomioiden mm. tunnistamisen vahvuus, roolien ja käyttäjäattribuuttien tarkkuus ja monimuotoisuus sekä pääsynhallinnan vahvuus, ks. alla) eri käyttäjäryhmille?

**Todentamisen vahvuustasot**

Käyttäjän todentamiseen liittyen on päätettävä mm. seuraavista todentamisen vahvuustasoista eri käyttäjäryhmille. On järkevää määritellä yhdenmukaisesti tasot ja kuhunkin todentamistasoon vastaavat ratkaisut, joista käyttäjäryhmä- ja/tai resurssikohtaisesti valitaan tarkemmin käytettävät. Karkeat todentamistasot voidaan määritellä esim. seuraavasti:

- vahva tunnistaminen: käyttäjän aitoudesta vahvistutaan ainakin kahdella eri todentamistavalla, esimerkiksi toimikortti ja salasana tai biometrinen tunnistus ja
- yksinkertainen tunnistautuminen esimerkiksi käyttäjätunnus/salasanaparin tai pelkän toimi- tai avainkortin avulla,
- anonyymikäyttö, ei tunnistautumista tai todentamista.

**Todentamistavat ja sessionhallinta**

Lisäksi on valittava, mitä todentamistapoja tuetaan, ja pyritäänkö todentamistavat yhtenäistämään. Eri todentamistapoja ja niiden yhtenäistämistä varten on tehtävä mm. seuraavia linjauksia ja suunnittelupäätöksiä:

- mitkä ovat käytettävät tunnistuksen menettelyt eri käyttäjäryhmille ja miten niitä yhdistellään esimerkiksi vahvaa tunnistamista varten?
- missä määrin pyritään käyttämään yhteisiä ja vain kerran toteutettuja tunnistamispalveluita, missä määrin hyväksytään järjestelmäkohtaiset tunnistautumistavat?
- miten laajasti pyritään saavuttamaan kertakirjautuminen eri järjestelmien ja palvelujen välillä?
- miten laajasti pyritään saavuttamaan yhdenmukaiset käyttäjätunnukset tai käyttäjien tunnisteet eri järjestelmien ja palvelujen välillä?
- kuinka voimassa oleva tunnistautuminen ja todentautuminen (sessio) säilytetään ja välitetään esimerkiksi kertakirjautumisympäristössä?

- kuinka monta erilaista sessiotasoa käyttäjille tarvitaan (esim. yhtäaikaa voimassaolevat adsisäänkirjautuminen, SSO-piirin sisäänkirjautuminen, sovelluskohtainen sisäänkirjautuminen)?
- kuinka tieto uloskirjautumisesta tai session päättymisestä välitetään sessioon kuuluville palveluille tai sovelluksille?
- onko käyttötilanteita, joissa käyttäjä on todennettava uudelleen tai tarkemmin kuin alkuperäinen tunnistautuminen?
- erotetaanko toisistaan yleisen esim. käyttöjärjestelmätason ja eri sovellusten käyttöä varten tapahtuva tunnistautuminen ja todentaminen?

Olemassaolevat sovellukset voivat aiheuttaa rajoitteita monien edellä kuvattujen seikkojen optimoinnille. Olennaista on myös pyrkiä erottamaan tunnistaminen ja todentaminen pääsynvalvonnasta.

**Roolimäärittelyjen suunnittelupäätöksiä**

Roolipohjainen käyttäjähallintamalli on yleinen ja suositeltava tapa käyttäjä- ja käyttövaltuushallinnan toteuttamiseen. Seuraavat kysymykset ohjaavat roolimäärittelyjen suunnittelua ja toteuttamista.

- määritelläänkö käyttäjärooleja useilla tasoilla, esim.
  - työrooli (esim. työrooli tai tehtävänimike ohjaa suoraan suuren osa käyttövaltuuksista)
  - yhteinen järjestelmärooli (useita sovelluksia tai palveluja kattava käyttövaltuuksien määrittely)
  - sovelluskohtainen järjestelmärooli (sovelluskohtaiset käyttöoikeudet)
- mitkä edellä kuvatuista tasoista otetaan keskitetyn roolimäärittelyn ja käyttäjähallinnan piiriin?
- mitkä ovat edellä kuvattujen tasojen väliset yhteydet ja tarvittavat toimenpiteet niiden yhdistämiseksi?
- onko tarvetta roolipohjaisen määrittelyn lisäksi käyttää myös suoraan käyttäjiin liitettäviä käyttövaltuuksien määrittelyjä?
- mitkä ovat keskeiset roolin tiedot?

**Keskityksen tavoitetaso ja master data management**

Keskeisiä käyttäjä- ja pääsynhallinnan tietovarantoja ovat:

- käyttäjähakemistot
- käyttäjätiedot (käyttäjätunnisteet, käyttäjätunnukset, salasanat, käyttäjätilien tiedot, käyttäjän roolit)
- roolitiedot (työroolit, yhteiset tai sovelluskohtaiset järjestelmäroolit)
- suojattujen resurssien tiedot
- käyttövaltuuksien tiedot (käyttäjiä, rooleja ja resursseja koskevat sekä mahdollisia muita valtuuksien päättelyyn tarvittavia tietoja)

Kunkin tietoryhmän osalta on tehtävä mm. seuraavia päätöksiä:

- kuinka monessa paikassa tietoa säilytetään

- onko tiedolla yksi master-järjestelmä tai palvelu
- mihin muihin järjestelmiin tiedot välitetään master-järjestelmästä (provisiointi) ja mikä on välittämistapa (kysely, automaattinen kopiointi tietovarastoihin tai käyttäjätietokantaan, manuaalinen kopiointi jne.)
- onko provisiointi yksi- vai kaksisuuntaista
- yhtenäistetäänkö tietojen säilytysratkaisut esim. pääkäyttäjäryhmien mukaisesti

Esimerkiksi käyttäjätunnusten hallinnan tehostamisen osalta voidaan pyrkiä keskittämisessä eri tasoihin (VIRTU 2008):

- eri järjestelmiin erillään syötettävät avattavista tunnuksista pyritään tekemään (manuaalisesti) samanmuotoisia,
- käyttäjätunnusten avaaminen tai sulkeminen tehdään keskitetysti, mutta esim. eri järjestelmissä säilyvät eri salasanat,
- edellisen lisäksi myös salasanat synkronoidaan järjestelmien välillä,
- on vain yksi käyttäjätunnus kutakin käyttäjää kohti.

**Käyttövaltuuksien tarkistamisen suunnittelupäätöksiä**

Käyttövaltuuksien tarkistamisen suhteen on päätettävä yleisesti mm. seuraavia asioita:

- missä määrin pyritään saamaan aikaan yhtenäinen tapa käyttövaltuuksien tarkistamiseen eri sovellusten, resurssien tai palvelujen käytössä?
- hyödynnetäänkö käyttövaltuuksien tarkistamiseen **yhteisiä tai keskitettyjä komponentteja** vai nojaudutaanko siihen, että tarvittavat käyttäjätiedot välitetään hajautetusti eri sovelluksiin tai palveluihin, jotka tekevät niiden pohjalta käyttövaltuuspäätöksen?
- nojaudutaanko käyttövaltuuksien tarkistamisessa **käyttäjätietoja sisältävän session** olemassaoloon ja miten sessiotieto on tällöin saatavissa?
- nojaudutaanko palvelupohjaisessa ympäristössä siihen, että infrastruktuurin tasolla (esim. SOAP header-tiedot) välitetään käyttäjä- tai käyttövaltuustietoja?
- onko käyttäjä-, käyttövaltuustietoja huomioitava SOA-palvelujen rajapinnoissa?
- mitkä seuraavista käyttöoikeuksien myöntämiseen liittyvistä tiedoista ovat tarpeen, ja mitkä niistä ratkaistaan yhteisten komponenttien, sessiotietojen välittämisen tai sovellus- tai palvelukohtaisten ratkaisujen avulla (pääsynhallinnan vahvuustasot):
    - käyttäjän yksilöinti ja todentaminen,
    - käyttäjän "kiinteät" roolitiedot, työrooli, yhteinen ja/tai sovelluskohtainen järjestelmärooli,
    - käyttäjän yksikkö,
    - käyttäjän muut attribuuttitiedot,
    - edustajuus - valtuutus käyttäjän toimimiseen toisen puolesta,
    - käyttökonteksti (esim. käyttöaika, sijainti, asiakassuhde / asiallinen yhteys, suostumus).
- mitkä yllä kuvatuista tiedoista ylläpidetään ja määritellään erillään toisistaan (tai tarkistetaan esim. erillisten palvelujen avulla)?

- mitkä yllä kuvatuista tiedoista syntyvät käyttäjän tunnistuksen ja todennuksen kautta?
- mitä yllä kuvatuista tiedoista on mahdollisissa yhteisesti saatavissa sessiotiedoissa?
- mitä yllä kuvatuista tiedoista selvitetään tilannekohtaisesti (pääsynvalvontatilanteessa) ja kenen vastuulla niiden selvittäminen on?

Käyttövaltuuksien tarkistamisessa on päätettävä resurssi-, sovellus- tai palvelukohtaisesti edellä mainittujen lisäksi mm. seuraavia asioita:

- mikä on resurssin, toiminnon tai palvelun suojaustaso, ja mihin rooleihin liittyen pääsy myönnetään?
- kenen vastuulla (mikä sovellus, palvelun kutsuja, palvelun tarjoaja, infrastruktuurissa sijaitseva välittäjä tai "vahti") on käyttövaltuuksien myöntämiseen liittyvien tietojen tarkastaminen (ks. yllä)?
- vaatiiko resurssin tai palvelun käyttö session tai käyttäjän todentamisen uudistamista?
- vaatiiko resurssin tai palvelun käyttö käyttökontekstin (ks. yllä) tarkistamista?

**SOA-ympäristöissä korostuvia suunnittelupäätöksiä**

Palvelupohjaisissa ratkaisuissa monet käyttäjähallinnan toiminnallisuudet voidaan toteuttaa itsekin SOA-palveluina (ks. luku 7). Tällöin saavutetaan yleisiä uudelleenkäyttö-, yhdenmukaisuus- ja joustavuusetuja, joita yleensäkin SOA-lähestymistavalla tavoitellaan. Lisäksi SOA-ympäristön arkkitehtuurissa voidaan huomioida mm. seuraavia seikkoja:

- SOA-palvelujen hyvänä suunnittelukäytäntönä voidaan pitää sitä, että käyttövaltuuksien tarkistukset ja käyttäjäsession ylläpito erotetaan toiminnallisiin ja tiedollisiin seikkoihin keskittyvien SOA-palvelujen rajapintamäärittelyistä, eli eivät ole osana palvelun varsinaisia rajapintoja. Tämä on mahdollista toteuttaa useilla tavoilla, mm. alla kuvatusti.
- Hallinnoidussa ja suojatussa kerroksittaisessa SOA-ympäristössä pääsynhallinta voidaan ainakin joiltain osin keskittää tiettyyn palvelu- tai käyttöliittymäkerrokseen, jolloin esim. integroivat portaalit tai edustasovellukset hoitavat käyttäjä- ja pääsynhallinnan ja taustalla olevat palvelut luottavat siihen, että vain valtuutetuilta sovelluksilta ja käyttäjiltä tulee palvelupyyntöjä, tai tunnistamiseen riittää suojattu yhteys tai pelkkä kommunikaation sovellusosapuolten tunnistaminen.
- Palvelujen väliseen kommunikointiin käytettävä palveluväylä (ESB) voi tarjota mahdollisuuksia käyttövaltuuksien toteuttamiseen ja valvontaan.
- Palvelujen suoritusympäristössä (mukaan lukien ESB tai web-sovelluspalvelimia suorittavat sovelluspalvelimet) on mahdollista toteuttaa arkkitehtuuri, jossa kutakin SOA-palvelua "vartioi" valvontapiste (Policy Enforcement Point), joka voi hyödyntää keskitetysti ylläpidettyjä käyttövaltuuksia ja käyttöpolitiikkaa esimerkiksi erillisen käyttövaltuuksien tarkistuspalvelun kautta (Policy Decision Point) (mm. Mathe ym. 2008). Käytännössä keskitettyjen käyttöpolitiikkojen (policy) hyödyntämisessä voidaan käyttää useita web services-tekniikoiden WS-laajennuksia sekä SAML-määrittelyjä, joiden avulla on mahdollista kuvata kaikki rooleihin, käyttäjien attribuutteihin sekä palvelujen käyttövaltuuksien määrittelyihin liittyvät rooli-, attribuutti- tai kontekstisidonnaiset säännöt. Luvun 7 palvelukuvauksissa ei ole erotettu yhtä policy-ratkaisua (esim. käyttöpolitiikkarekisteriä), vaan erilaisiin rajoitteisiin liittyvät seikat on kuvattu omina palveluinaan. Yksinkertainen avoimia WS-määrityksiä hyödyntävä policy-arkkitehtuuri olisi mahdollista toteuttaa esimerkiksi käyttövaltuushallintapalvelun, eri

palveluja (esim. käyttäjäprofiilipalvelu) käyttävän pääsynvalvontapisteen ja pääsynvalvontapalvelun avulla.

Käyttökelpoisia web services-suosituksia turvallisuuskontekstin luomisessa ovat mm. WS-SecureConversation, WS-Trust sekä identiteettien yhdistämisessä WS-Federation, sekä käyttöpolitiikkojen osalta WS-Policy ja WS-SecurityPolicy (Sormunen ym. 2007).

# 7 Käyttäjähallinnan SOA-palvelujen tunnistaminen ja rajaus

Tässä luvussa esitetään keskeisiä käyttäjä- ja käytönhallinnan palveluja järjestelmä- ja teknologiariippumattomasti. Tavoitteena on tunnistaa SOA-palveluja sekä rajapintatarpeita, joiden avulla käyttäjähallinnan ratkaisuja voidaan kehittää modulaarisesti ja joustavasti. Tehtyjen rajausten mukaisesti mm. lokit ja käytön hallinta sekä valmiiden IdM / IAM -ratkaisujen kattamat alueet käsitellään kevyemmin.

Tunnistetuista potentiaalisista palveluista kuvataan lyhyesti käyttötarkoitus ja päätoiminnallisuudet. Lisäksi keskeisimmistä palveluista ollaan tuottamassa tarkennettuja palvelukohtaisia palvelunkuvaustaulukoita, jotka toimivat pohjana tarkennetulle toiminnalliselle palvelumäärittelylle.

On huomioitava, että edellisessä luvussa esitettyjen suunnittelupäätösten pohjalta eri palveluilla voi olla yksi tai useampia toteutuksia tietyssä ympäristössä (palveluluettelossa ei tehdä oletuksia palvelujen lukumäärästä). Palvelut on tunnistettu osin valmiita malleja hyödyntäen, ja useat palveluista ovat usein nykytilanteessa samoissa sovelluksissa sijaitsevia tai sellaisia, että niihin liittyviä toiminnallisuuksia tai tietoja on toteutettu päällekkäisinä moniin eri järjestelmiin.

Palvelumäärittelyssä ei oteta kantaa siihen, onko palvelulla oma erikoistunut käyttöliittymä, vaan lähtökohtana on, että palvelua kutsutaan rajapinnan kautta, ja kutsuja voi olla toinen palvelu tai käyttöliittymäsovellus (esim. käyttäjähallintajärjestelmä, henkilöstöhallinnon sovellus, käyttäjä- tai valtuustietoja kyselevä sovellus).

Tunnistettujen palvelujen luettelosta voidaan valita palveluja ja toiminnallisuuksia, joita halutaan keskittää yhteisesti hoidettavaksi tai yhtenäistää. Samoin voidaan päättää, että jotkin palvelujen aiheista yhdistetään ja vaaditaan hankittavilta IdM-ratkaisuilta, tai yritetään saada integroitua hajautetusti useiden sovellusten tai palvelujen avulla (esim. yksiköittäin, sovelluksittain, käyttäjäryhmittäin).

**Käyttäjien, roolien ja valtuuksien määrittely**

| | |
|---|---|
| Käyttäjähallintapalvelu | toiminnallinen palvelu, joka tarjoaa käyttäjien käyttäjätilitietojen ylläpitotoiminnot (mm. käyttäjien lisääminen, poistaminen, käyttäjien käyttäjätili- ja attribuuttitietojen ylläpito) |
| Käyttövaltuushallintapalvelu | toiminnallinen palvelu, jolla käyttäjät ja käyttäjätilit yhdistetään rooleihin ja käyttöoikeuksiin |
| Roolienhallintapalvelu | toiminnallinen palvelu, jolla ylläpidetään roolitietoja, sisältää myös roolirekisterin |
| Resurssienhallintapalvelu | palvelu, jonka avulla määritellään suojattavat resurssit, sovellukset ja palvelut sekä niiden käyttöön tarvittavat valtuudet; voi liittyä käyttövaltuushallintapalveluun |
| Käyttäjähakemisto | hakemisto, joka tarjoaa pääsyn ainakin keskeisiin käyttäjähallintapalvelun kautta ylläpidettyihin tietoihin; hakemiston rajapintojen avulla voidaan kysellä käyttäjätietoja |
| Metahakemisto | hakemisto, joka yhdistää useiden muiden käyttäjä- tai henkilöhakemistojen tietoja ja sisältää niiden välisten suhteiden määrittelyt |
| Käyttövaltuusrekisteri | tietopalvelu, joka säilyttää ja palauttaa tiedon käyttäjien käyttövaltuuksista. |
| Provisiointipalvelut | palvelu, jonka avulla keskitetysti ylläpidetyt (master) käyttäjä- ja käyttövaltuustiedot voidaan levittää useisiin eri järjestelmiin; voi myös sisältää toiseen suuntaan tapahtuvaa käyttäjähallintatietojen välitystä |
| Federointipalvelu | toiminnallinen palvelu, jonka avulla käyttäjien erilliset identiteetit yhdistetään luottamusverkostossa |
| Käyttäjäprofiilipalvelu | palvelu, jonka kautta käyttäjän attribuutteja (mahdollisesti myös muuhun kuin pääsynhallintaan liittyen, esim. käyttäjäpreferenssit) voidaan ylläpitää ja saada niitä tarvitseville; voi olla joissakin tapauksissa yhdistettynä etenkin käyttäjähakemistoon tai käyttäjähallintapalveluun |
| Valtuutusten ja suostumusten hallintapalvelut | palvelut, joilla ylläpidetään tietoa käyttäjän tai asiakkaan antamista valtuutuksista tai suostumuksista |

Edellä kuvatuista palveluista monet voivat liittyä läheisesti toisiinsa: esimerkiksi käyttäjähallintapalvelu, käyttövaltuushallintapalvelu, roolienhallintapalvelu, käyttövaltuusrekisteri sekä käyttäjäprofiilipalvelu ovat tyypillisiä IdM/IAM-ratkaisuihin sisältyviä toiminnallisuuksia. SOA-pohjaisessa arkkitehtuurissa ne ovat kuitenkin erotettavissa myös erillisiksi palveluiksi tai rajapinnoiksi, mikäli esim. vähittäisen siirtymän tai hajautusmallin kannalta tämä on tarkoituksenmukaista. Myös resurssienhallintapalvelu on mahdollista erottaa käyttövaltuuksienhallintapalvelusta esimerkiksi, mikäli niissä käytetään yhtenäistä tietomallia.

**Käyttäjien tunnistaminen ja todentaminen**

| | |
|---|---|
| Tunnistuspalvelu (sisäinen tunnistuspalvelu) | toiminnallinen palvelu, jonka avulla oman organisaation käyttäjä voi tunnistautua (tekee tunnistamisen ja todentamisen), ja joka palauttaa käyttäjän identiteetin sekä mahdollisesti tunnistusselosteen ja muita sovittuja käyttäjän attribuutteja |
| Asiakkaan tunnistuspalvelu | tunnistuspalvelu, joka on tarkoitettu organisaation ulkoisten asiakkaiden tunnistamiseen, usein yleiskäyttöinen ja kansalaiskeskeinen |
| Federoitu tunnistuspalvelu | käyttäjän kotiorganisaatiossa sijaitseva tunnistuspalvelu, joka palauttaa tunnistusselosteen / tunnistustiedot palveluntarjoajalle (palvelujärjestelmän omistaja ja ylläpitäjä) |
| Todentamispalvelu | palvelu, joka vahvistaa tunnistetun käyttäjän aitouden tarvittaessa lisätarkistuksia tai tunnistuksia tehden |
| Kertakirjautumispalvelu | palvelu, jonka avulla voidaan kirjautua kerralla sisään (tunnistautua ja todentautua) useisiin palvelun piirissä oleviin järjestelmiin |
| Sessionhallintapalvelu | palvelu, joka säilyttää ja välittää tiedon voimassa olevasta käyttäjäsessiosta ja siihen liittyvistä tiedoista sekä session tietojen muuttumisesta sekä session päättymisestä |

**Pääsynvalvonta**

| | |
|---|---|
| Pääsynvalvontapalvelu | palvelu, joka ottaa vastaan käyttäjätietoja ja muita käyttöoikeuksien päättelyyn tarvittavia tietoja ja palauttaa tiedon siitä myönnetäänkö resurssin käyttöön valtuudet |
| Pääsylokipalvelut | palvelut, jotka keräävät pääsynvalvonnan alaisten resurssien, palvelujen ja sovellusten käytön seurantatietoja; lokipalvelut voivat erikoistua tietyntyyppisten lokien käsittelyyn (VAHTI 2008) |
| Käytön raportointipalvelu | palvelu, joka etenkin lokipalveluihin liittyen tuottaa yhteenvetoja ja raportteja käytöstä |
| Kontekstipalvelut (dynaamisten attribuuttien hakupalvelut) | palvelu, joka tarvittaessa palauttaa tiedon voimassa olevasta käyttökontekstista (mukaan lukien tietoja joita saatetaan tarvita pääsynvalvonnassa) - voi myös eriytyä erillisiksi palveluiksi, esim. sijainti, asiayhteyden päättely, suostumuksen tarkistaminen (huom. erotettu roolipalvelusta) |
| Roolipalvelu | palvelu, joilla selvitetään käyttäjien roolitietoja (voi sisältää mm. organisaatio, valtuutus, työrooli, järjestelmäroolit, perhesuhteet, kuntalaisuus, kansalaisuus). huom. erotettu tässä muusta toimintakontekstista (kontekstipalvelut); ks. myös käyttäjäprofiilipalvelu |
| Pääsynvalvontapiste | palvelu, joka "vartioi" suojattua resurssia tai palvelua ja sille tulevia palvelu- tai hakupyyntöjä, ja voi erottaa viestinnästä tai tuntemastaan sessiosta tai muista tiedoista käyttövaltuuspäätöksien tekemiseen tarvittavia tietoja, suorittaa itse tai hyödyntämällä pääsynvalvontapalveluja käyttövaltuuksien arvioinnin sekä joko myöntää pääsyn resurssiin tai palveluun tai estää sen. |

Pääsynvalvontapalvelun kutsumiseksi voi olla tarpeen koota tarvittavia tietoja esim. voimassa olevasta sessiosta, käyttäjähakemistosta tai käyttäjäprofiilipalvelusta ja kontekstipalvelusta. Edelleen useat palvelut voivat sijaita yhdessä: esimerkiksi terveydenhuollossa käytetyt kontekstinhallintarat-

kaisut sisältävät sekä sessionhallintapalvelun, kontekstipalvelun että kertakirjautumispalvelun ominaisuuksia.

Tehdyt rajaukset huomioiden keskeisimmät ensi vaiheessa tarkennetuiksi palveluiksi on tässä vaiheessa ehdotettu pääsynvalvontapalvelu, käyttäjähakemisto, käyttövaltuusrekisteri sekä tunnistamis- ja sessionhallintapalvelut. Näiden välisten pelisääntöjen tarkennuksella saadaan aikaan perusarkkitehtuuripäätökset myös palvelupohjaisen pääsyn- ja käytönhallinnan tarkennukselle.

Mainituista palveluista on tuotettu tarkempia palvelunkuvaustaulukoita, ja tarkennettu palveluiden vastuiden ja rajapintatoiminnallisuuksien lisäksi yhteisesti mm. luvun 6 suunnittelupäätöksiä. Lisäksi olennaista on tarkentaa keskeisten palvelujen yhteistä tietoarkkitehtuuria (mm. tunnisteet, yhteisesti sovittavat attribuutit, eri tietokokonaisuuksien lähteet ja käyttäjät jne.).

# 8 Palvelukuvaustaulukot

Palvelukuvaustaulukoissa on esitetty palvelut seuraavien mm. tässä dokumentissa esitettyjen luokitusten ja jaotteluiden sekä muiden palveluita kuvaavien ominaisuuksien (taulukon rivit) avulla:

- *Palvelun nimi:* palvelun kuvaava ja yksilöivä nimi
- *Tarkoituksen lyhyt kuvaus: mitä toimintoja ja tietoja kattaa*: kuvaus palvelun perustoiminnallisuudesta, toimintojen ja tietojen kuvaus yleisesti esim. "tunnusten hakeminen hakusanojen avulla"
- *Keskitys/hajautus*: esitys/arvio palveluiden infrastruktuurimallista
- *Mihin prosessiin / tehtävään liittyy*: missä luvussa 5 esitetyissä prosesseista palvelu on osana
- *Mihin sovelluksiin / tuotteisiin liittyy*: useat palveluista ovat paketoitu osaksi eri tuoteratkaisuja, esim. missä tuotteista kyseinen tai vastaava ratkaisu on saatavilla (yleisnimi tuotteelle, kuten LDAP-hakemisto)
- *Mihin määrityksiin liittyy*: tunnistettuja standardeja, määrityksiä tai valmiita malleja, joita voidaan hyödyntää sinällään tai pohjana palvelun määrityksessä liittyen palvelun toiminnallisuuteen tai sen hyödyntämiin tietoihin
- *Yhteydet ja riippuvuudet muihin palveluihin:* muut palvelut, joihin kyseinen palvelu on kutsusuhteessa osana toiminnallisuuttaan, esim.: Tämä tarvitsee taakseen/kutsuu palvelua
- *Arvio saatavuudesta / toteutettavuudesta / mukauttamistarpeista:* arvio toteutusten saatavuudesta, esim. ostettavissa tuotteena, toteutettavissa määrityksen pohjalta tms.
- *Muut kommentit:* muuta huomionarvoista palvelusta
- *Käyttäjätyyppiluokka*: minkä käyttäjätyyppien käsittelyyn liittyy (kts. luku 4 – Taulukko): ”organisaation hallinnoimat käyttäjät / työntekijät”, asiakas- tai kansalaiskäyttäjät, kumppaniorganisaatioiden hallinnoimat käyttäjät (luottamusverkosto) tai esim. "kaikki luokat"
- *Päätoimintoluokka*: mihin toimintoluokkaan palvelu pääasiallisesti kuuluu (kts. luku 7): ”Käyttäjien, roolien ja valtuuksien määrittely”, ”Käyttäjien tunnistaminen ja todentaminen” tai ”Pääsynvalvonta”

## 8.1 Tunnistuspalvelu

| | |
|---|---|
| Palvelun nimi | Tunnistuspalvelu (sisäinen tunnistuspalvelu) |
| Tarkoituksen lyhyt kuvaus: mitä toimintoja ja tietoja kattaa | Toiminnallinen palvelu, jonka avulla oman organisaation käyttäjä voi tunnistautua (tunnistaminen ja todentaminen)<br>**Toiminnot:**<br>palauttaa käyttäjän identiteetin sekä mahdollisesti tunnistusselosteen ja muita sovittuja käyttäjän attribuutteja tunnistetietojen perusteella.<br>Voi toimia yhdessä mm. kertakirjautumispalvelun ja sessiopalvelun kanssa. |
| Keskitys / hajautus | Nykytila: tunnistautuminen usein sovelluskohtaista.<br>Tavoitetila: keskitettyjen tunnistuspalvelujen käytön lisääminen, optimina yksi tunnistuspalvelu / organisaatio. |
| Mihin prosessiin / tehtävään liittyy | 2.1 tunnistautuminen, sisältäen tunnistetietojen esittämisen, tunnistamisen ja todentamisen<br>2.2 käyttäjän todentaminen, ilman tunnistetietojen erillistä esittämistä<br>2.3 sisäänkirjautuminen järjestelmään (automatisoitu esim. kertakirjautumisen yhteydessä, tai tunnistautumisen sisältävä)<br>2.4 uloskirjautuminen järjestelmästä (mikäli sekä sisäänkirjautuminen että uloskirjautuminen hoidetaan palvelun kautta)<br>2.5 käyttäjän vaihto (sisältäen uloskirjautumisen ja sisäänkirjautumisen)<br>2.6 sähköinen allekirjoitus (voi hyödyntää samaa tunnistamis/todentamisinfrastruktuuria) |
| Mihin sovelluksiin / tuotteisiin liittyy | Tavoitetilassa monet käyttäjän työpöytäsovellukset ja eri resurssien käyttö nojautuvat nykyistä keskitetympään tunnistuspalvelujen käyttöön. |
| Mihin määrityksiin liittyy | SAML ID Provider, TUPAS, Ydinpalvelurajapinnat, OpenID, EUA, |
| Yhteydet ja riippuvuudet muihin palveluihin | Voi kutsua seuraavia: Todentamispalvelu (mikäli erillinen), Sessionhallintapalvelu ja Kertakirjautumispalvelu (jos asettaa sessiotietoja)<br>Seuraavat palvelut voivat kutsua palvelua: Federoitu tunnistuspalvelu (joka voi nojautua paikallisen tunnistuspalvelun toimintaan), Sessionhallintapalvelu ja kertakirjautumispalvelu (mikäli arkkitehtuurissa tunnistautuminen hoidetaan sessionhallinnan kautta) |
| Arvio saatavuudesta / toteutettavuudesta / mukauttamistarpeista | Nykyisin useita sovelluskohtaisia tunnistusratkaisuja. Myös yhteiskäyttöisiä tunnistuspalveluja saatavilla organisaatioiden sisäiseen käyttöön/ulkoisia tunnistuspalveluja. Vaatii integroinnin sovelluksiin, jotka nojautuvat palvelun käyttöön. |
| Muut kommentit | |
| Käyttäjätyyppiluokka | organisaation hallinnoimat käyttäjät / työntekijät |
| Päätoimintoluokka | käyttäjien tunnistaminen ja todentaminen |

## 8.2 Käyttäjähakemisto

| | |
|---|---|
| Palvelun nimi | Käyttäjähakemisto |
| Tarkoituksen lyhyt kuvaus: mitä toimintoja ja tietoja kattaa | Hakemiston rajapintojen avulla voidaan kysellä käyttäjätietoja (käyttäjätunnisteet, käyttäjätunnukset, salasanat, käyttäjätilien tiedot, käyttäjän roolit).<br>**Toiminnot:**<br>palauttaa käyttäjän identifioivan tiedon perusteella kysytyt käyttäjään liittyvät tiedot. |
| Keskitys / hajautus | Nykytila: tyypillisesti käyttäjähakemistoja eri tasoilla, sovellusten sisäisiä käyttäjähakemistoja<br>Tavoitetila: yleensä master-käyttäjähakemiston käyttöönotto, erillisten käyttäjähakemistojen vähentäminen |
| Mihin prosessiin / tehtävään liittyy | 1.9 käyttäjätilin lisääminen<br>1.11. käyttäjätilin poistaminen tai disablointi<br>1.12. työ- ja järjestelmäroolien ylläpito (määrittely, lisääminen, valtuuksien määrittely, poistaminen)<br>1.13. käyttäjätietojen provisiointi esim. keskitetystä käyttäjähallintavarastosta<br>1.14. salasanan vanhentuminen<br>1.15. salasanan vaihtaminen<br>1.16. yhdistetyn käyttäjäidentiteetin ylläpito<br>2.1 tunnistautuminen, sisältäen tunnistetietojen esittämisen, tunnistamisen ja todentamisen |
| Mihin sovelluksiin / tuotteisiin liittyy | esim. LDAP-hakemisto |
| Mihin määrityksiin liittyy | SAML ID Provider ja Security Token Service, LDAP, Ydinpalvelurajapinnat, OpenID |
| Yhteydet ja riippuvuudet muihin palveluihin | Ei kutsu muita palveluja.<br>Palvelua kutsutaan, kun tarvitaan tai päivitetään hakemiston käyttäjätietoja (useat muut palvelut ja ylläpitosovellukset). |
| Arvio saatavuudesta / toteutettavuudesta / mukauttamistarpeista | hakemistoja valmiina tuotteita saatavilla ja paketoituna esim. osaksi IdM-tuotteita, |
| Muut kommentit | |
| Käyttäjätyyppiluokka | kaikki käyttäjät, mahdollisesti eri hakemistoja eri käyttäjätyypeille |
| Päätoimintoluokka | käyttäjien ja roolien määrittely |

## 8.3 Pääsynvalvontapalvelu

| Palvelun nimi | Pääsynvalvontapalvelu |
|---|---|
| Tarkoituksen lyhyt kuvaus: mitä toimintoja ja tietoja kattaa | palvelu, jonka avulla **järjestelmän** tai sen osien käyttö mahdollistetaan vain valtuutetuille **käyttäjille.** Palvelu ottaa vastaan käyttäjän identiteettitiedon ja tiedon resurssista tai palvelusta, johon pääsyä tarvitaan. Muiden käyttäjätietojen ja käyttöoikeuksien päättelyyn tarvittavien tietojen hakemiseen voidaan hyödyntää muita palveluja. Palauttaa tiedon siitä myönnetäänkö resurssin käyttöön oikeudet.<br>**Toiminnot:**<br>palauttaa tiedon siitä myönnetäänkö resurssin käyttöön oikeudet<br>resurssi- ja käyttövaltuustietojen perusteella |
| Keskitys / hajautus | Nykytila: yhteinen pääsynvalvonta nojautuu tyypillisesti sovelluskohtaisiin ratkaisuihin ja on karkeajakoista (esim. sovellustaso). Hienojakoinen pääsynvalvonta toteutettu sovelluksiin.<br>Tavoitetila tyypillisesti: yhteisen pääsynvalvonnan tarkkuuden lisääminen ja yhdenmukaistaminen, esim. sovellusten käynnistyksen tai resurssipyyntöjen yhteydessä keskitetyn palvelun hyödyntäminen, tai hajautettujen pääsynvalvontapisteiden kautta tapahtuva pääsynvalvonta. |
| Mihin prosessiin / tehtävään liittyy | 3.2. käyttäjäprofiilin perusteella tehtävä käyttövaltuustarkastus<br>3.3. käyttäjäprofiiliin kuuluvien roolitietojen (työrooli, järjestelmärooli) perusteella tehtävä käyttövaltuustarkastus<br>3.4. käyttökontekstitietojen (esim. sijainti, aika, asiakassuhde, suostumus) perusteella tehtävä käyttövaltuustarkastus<br>3.5. käyttäjän session voimassaolon tarkastaminen (mikäli tehdään sessionhallintaan liittyen)<br>3.6. resurssin käyttöön liittyvän käyttöpolitiikkamäärityksen (policy) noutaminen ja evaluointi suhteessa käyttäjäprofiili- ja käyttökontekstitietoihin |
| Mihin sovelluksiin / tuotteisiin liittyy | Päätettävä sovelluskohtaisesti, mille tasolle pääsynvalvonta viedään, esim. sovelluksen käynnistys, sovelluksen toimintojen tai sen tarvitsemien resurssien pääsynvalvonta. |
| Mihin määrityksiin liittyy | SAML, XACML, RAD, Ydinpalvelurajapinnat, WS-Policy- ja WS-SecurityPolicy |
| Yhteydet ja riippuvuudet muihin palveluihin | Perussyötteitä palvelun käyttöön identiteetti ja tieto resurssista. Suunnittelupäätös: 1) miltä osin mahdollisesti tarvittavat konteksti-, rooli-, sessio- ym. tiedot tulevat mukana pääsynvalvontapalvelun kutsussa vai 2) selvittääkö palvelu ko. tiedot.<br>Palvelua voi kutsua: Pääsynvalvontapiste<br>Palvelu voi kutsua: Käyttövaltuusrekisteri, Kontekstipalvelu (2), Roolipalvelu (2), Sessionhallintapalvelu (2) |
| Arvio saatavuudesta / toteutettavuudesta / mukauttamistarpeista | Työläs lisätä vanhoihin sovelluksiin hienojakoisella tasolla. Palvelupohjaisessa ympäristössä määriteltävä yhtenäinen pääsynvalvonta-arkkitehtuuri, ks. käyttövaltuuksien hallinnan suunnittelupäätökset. |
| Muut kommentit | |
| Käyttäjätyyppiluokka | kaikki käyttäjät |
| Päätoimintoluokka | Pääsynvalvonta |

## 8.4 Käyttövaltuusrekisteri

| | |
|---|---|
| Palvelun nimi | Käyttövaltuusrekisteri |
| Tarkoituksen lyhyt kuvaus: mitä toimintoja ja tietoja kattaa | Tietopalvelu, joka säilyttää ja palauttaa tiedon käyttäjien käyttövaltuuksista (käyttäjiä, rooleja ja resursseja koskevat sekä mahdollisia muita valtuuksien päättelyyn tarvittavia tietoja)<br>**Toiminnot:** palauttaa käyttäjän (ja tai roolin) identifioivan tiedon perusteella tiedot käyttövaltuuksista.<br>Käyttövaltuuksien ylläpitotoiminnot. |
| Keskitys / hajautus | Nykytila: yhteiskäyttöisiä / keskitettyjä käyttövaltuusrekisterejä vähän tai erillisiin käyttötarkoituksiin.<br>Tavoitetila: master-käyttövaltuusrekisteri keskeisille käyttövaltuustiedoille organisaatiossa. |
| Mihin prosessiin / tehtävään liittyy | 1.5. käyttövaltuuksien puoltaminen ja hyväksyminen<br>1.6. käyttövaltuuksien poisto<br>1.7. edustajuuden (toisen puolesta toimiminen) ylläpito<br>1.10. käyttäjän valtuuksien määrittely / liittäminen järjestelmärooleihin<br>1.11. käyttäjätilin poistaminen tai disablointi<br>1.12. työ- ja järjestelmäroolien ylläpito (määrittely, lisääminen, valtuuksien määrittely, poistaminen)<br>2.3. sisäänkirjautuminen järjestelmään<br>2.5 käyttäjän vaihto<br>3.3 käyttäjäprofiilin perusteella tehtävä käyttövaltuustarkastus-käyttäjäprofiiliin kuuluvien roolitietojen (työrooli, järjestelmärooli) perusteella tehtävä käyttövaltuustarkastus<br>3.6 resurssin käyttöön liittyvän käyttöpolitiikkamäärityksen (policy) noutaminen ja evaluointi suhteessa käyttäjäprofiili- ja käyttökontekstitietoihin<br>3.7 resurssien käyttöön tarvittavien käyttäjä-, rooli- ja kontekstitietojen määrittely ja ylläpito (toiminnot) |
| Mihin sovelluksiin / tuotteisiin liittyy | Käyttäjähakemisto-, IdM- ja IAM-tuotteet, palvelinten, hallittujen ympäristöjen (esim. AD) ja sovellusten käyttäjähallinta. |
| Mihin määrityksiin liittyy | XACML, Ydinpalvelurajapinnat |
| Yhteydet ja riippuvuudet muihin palveluihin | Ei kutsu tyypillisesti muita palveluja.<br>Käyttövaltuuksien kyselyn yhteydessä |
| Arvio saatavuudesta / toteutettavuudesta / mukauttamistarpeista | Pääosin IAM-tuotteiden kattamaa toiminnallisuutta, tietojen saatavuusrajapinnat olennaisia. |
| Muut kommentit | |
| Käyttäjätyyppiluokka | kaikki käyttäjät |
| Päätoimintoluokka | käyttäjien ja roolien määrittely |

## 8.5 Sessionhallintapalvelu

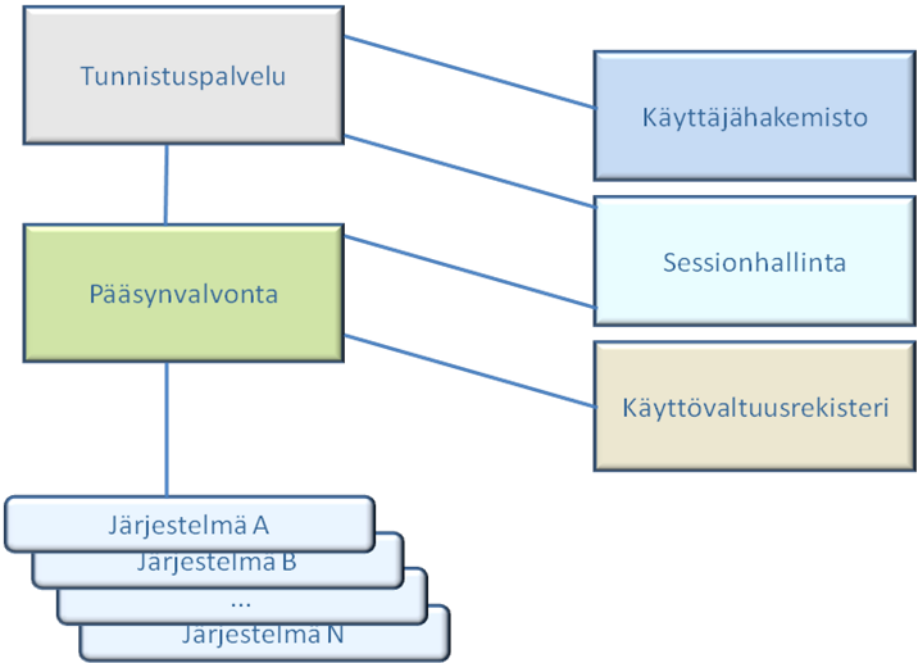
| | |
|---|---|
| Palvelun nimi | Sessionhallintapalvelu |
| Tarkoituksen lyhyt kuvaus: mitä toimintoja ja tietoja kattaa | palvelu, joka säilyttää ja välittää tiedon voimassa olevasta käyttäjäsessiosta ja siihen liittyvistä tiedoista sekä session tietojen muuttumisesta sekä session päättymisestä |
| Keskitys / hajautus | Valittava, mihin eri sessioihin hyödynnetään yhteisiä malleja (esim. käyttöjärjestelmän kirjautuminen, luotetun sovellusympäristön sisäänkirjautuminen, web-sessio). Eri vaihtoehdoissa valittavissa hajautettuja (esim. työasemalla / selaimessa säilytettävä sessiotieto) tai keskitettyjä (sessiopalvelu, kontekstinhallintapalvelu) vaihtoehtoja. |
| Mihin prosessiin / tehtävään liittyy | 2.1 tunnistautuminen, sisältäen tunnistetietojen esittämisen, tunnistamisen ja todentamisen<br>2.2 käyttäjän todentaminen, ilman tunnistetietojen erillistä esittämistä<br>2.3 sisäänkirjautuminen järjestelmään (automatisoitu esim. kertakirjautumisen yhteydessä, tai tunnistautumisen sisältävä)<br><br>2.4 uloskirjautuminen järjestelmästä<br><br>2.5 käyttäjän vaihto (sisältäen uloskirjautumisen ja sisäänkirjautumisen)<br><br>3.5 käyttäjän session voimassaolon tarkastaminen (mikäli tehdään sessionhallintaan liittyen) |
| Mihin sovelluksiin / tuotteisiin liittyy | Hallittu käyttöjärjestelmäympäristö (esim. AD), kertakirjautumissovellukset, web-sovellukset ja portaalit, kertakirjautumiseen liittyvät sovellukset. |
| Mihin määrityksiin liittyy | TUPAS, minimikontekstinhallinta, Ydinpalvelurajapinnat |
| Yhteydet ja riippuvuudet muihin palveluihin | Voi toimia yhdessä tunnistuspalvelujen kanssa - valittava kumpi ohjaa toimintaa. Pääsynvalvonta voi tarvita sessionhallintapalvelun tietoja. |
| Arvio saatavuudesta / toteutettavuudesta / mukauttamistarpeista | Eri sessiotasoille erityyppisiä ratkaisuja valmiina ja saatavilla, valittava arkkitehtuurissa yhteisesti hyödynnettävät tavat. |
| Muut kommentit | |
| Käyttäjätyyppiluokka | organisaation hallinnoimat käyttäjät / työntekijät, asiakas- tai kansalaiskäyttäjät |
| Päätoimintoluokka | Käyttäjien tunnistaminen ja todentaminen |

## 8.6 Kuvattujen palveluiden yhteistoiminta

Kuvassa 1 on esitetty periaatteellinen malli hyödynnettäväksi jatkossa tehtävälle tarkemmalle arkkitehtuurin määritystyölle kuvattavaksi valituista palveluista (luvut 8.1.- 8.5):

- Tunnistuspalvelu,
- Pääsynvalvonta,
- Käyttäjähakemisto,
- Käyttövaltuusrekisteri,
- Sessionhallinta

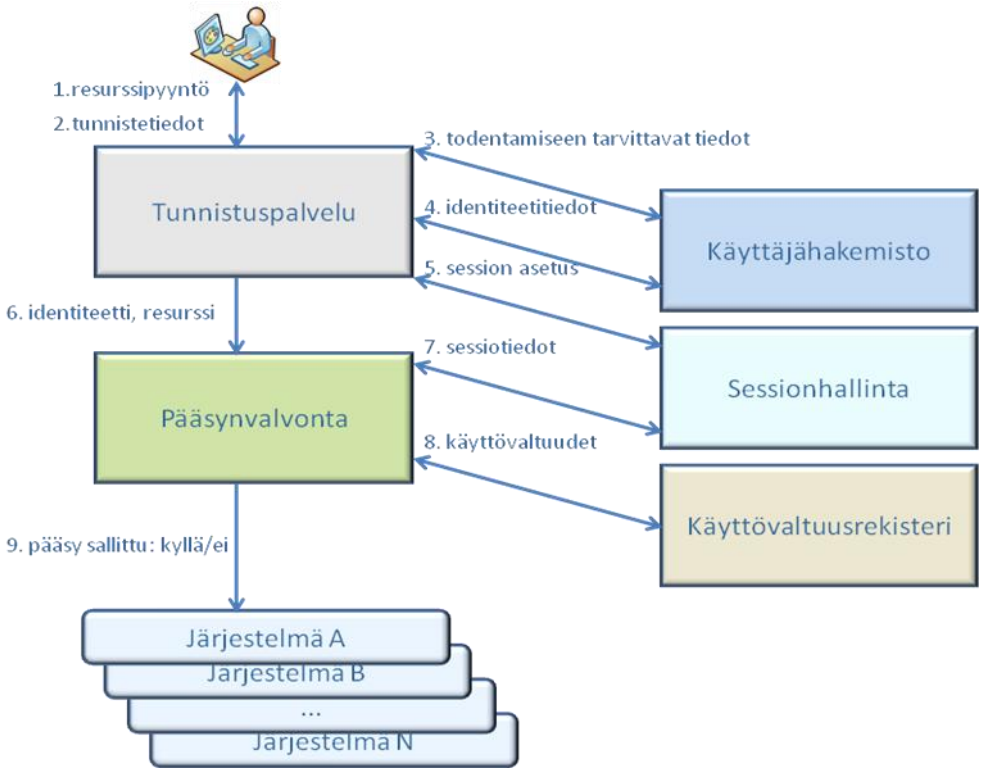
sekä esitetty myös palveluiden väliset yhteydet ja pääsynvalvonnan liityntä olemassa oleviin järjestelmiin.




**Kuva 1**. Tarkasteltaviksi valittujen palveluiden väliset suhteet

Palveluiden välistä mahdollista yhteentoimivuusmallia havainnollistamaan on laadittu myös Kuvassa 2 esitetty tyypillinen suorituksen eteneminen (Käyttäjän sisäänkirjautuminen ja valvottuihin järjestelmään pääsy), jossa lisätty Kuvan 1 pohjaan käyttäjä sekä palveluiden välillä hyödynnetyt tiedot. Kuvaus esittää yhden esimerkin palveluiden loogisesta kutsumisjärjestyksestä, joka esittelee palveluiden välisiä kutsuja ja kutsuissa käytettyjä tietoja. Kuvaus ei kuitenkaan esitä esim. tietopalveluiden Käyttäjähakemisto- ja Käyttövaltuusrekisteri-palveluiden ylläpitorajapintojen hyödyntämistä, mitkä eivät tule vastaan tai tunnistetuiksi palveluiden operatiivisen käytön kuvauksissa. Vastaavien tyypillisten suoritusten (toimintoketjun/käyttötapauksen) kuvaamisen avulla voidaan tunnistaa myös muunlaisia malleja palveluiden ja niiden tietojen hyödyntämiselle sekä palveluiden välisille kutsusuhteille. Tämän yleisen kuvan tarkentaminen kannattakin tehdä paikallisten tarpeiden ja mahdollisesti valmiina hyödynnettävien mallien (ks. luku 9) pohjalta.

Kuvauksen kulku on pidetty yhdenmukaisena VAHTI-ohjeessa (VAHTI 2006) esitetyn ”Käyttäjien tunnistaminen ja pääsynvalvonta”-kuvauksen kanssa, esittäen suorituksen etenemisen tässä dokumentissa esitettyjen palvelutoteutuksia hyödyntäen.




**Kuva 2**. Palveluiden välinen yhteistoiminta selvitetty tyypillisellä työnkululla (käyttäjän kirjautuminen ja pääsy järjestelmään)

Kuvassa 1 esitettyjä palveluiden välisiä kutsusuhteita on havainnollistettu Kuvassa 2 lisäämällä kutsut, kutsujärjestys ja kutsujen tietosisältö suhteessa esitettyyn työnkulkuun:

1. Resurssipyyntö: esim. käyttäjä käynnistää sovelluksen (huom. tyypillisesti edeltävä vaihe: Pääsynvalvonta uudelleenohjaa resurssipyynnöt sisäänkirjautumattomilta käyttäjiltä Tunnistuspalvelulle)
2. Tunnistetiedot: koska käyttäjä ei ole vielä kirjautunut sisään Tunnistuspalvelu pyytää käyttäjältä tunnistetiedot (esim. sisäänkirjautumisdialogilla annettavat käyttäjätunnus, salasana)
3. Saatuaan tunnistetiedot Tunnistuspalvelu tarkastaa tiedot Käyttäjähakemiston tallettamia tietoja vasten (esim. hakee annettua käyttäjätunnusta vastaavan salasanan)
4. Tunnistetietojen ollessa kunnossa hakee Tunnistuspalvelu Käyttäjähakemistosta käyttäjän identiteettitiedot (esim. SAML-tunnisteseloste)
5. Tunnistuspalvelu asettaa käyttäjän sessiotiedot Sessionhallintapalveluun
6. Tunnistuspalvelu välittää eteenpäin Pääsynvalvontapalvelulle käyttäjä identiteettitiedot ja pyydetyn resurssin tiedot (esim. järjestelmään pääsy)
7. Pääsynvalvontapalvelu hakee käyttäjäidentieettiin liitetyt käyttövaltuudet suhteessa pyydettyyn resurssiin Käyttövaltuusreksiteristä (esim. policyt, XACML)
8. Pääsynvalvontapalvelu varmistaa Sessionhallintapalvelulta, että myös käyttäjän istunto on voimassa (esim. hakemalla ja tarkistamalla sessiotiedon).
9. Jos Pääsynvalvontapalvelun tarkistamat oikeudet ovat kunnossa käyttäjälle sallitaan pääsy haluttuun resurssiin (esim. välittämällä mm. identiteettitiedot ja haluttu resurssipyyntö ko. järjestelmälle)

# 9 Valmiita malleja

Vaikka pääasiallinen käyttäjähallinnan jäsentäminen tapahtuu toiminta- ja prosessilähtöisesti, on tähän lukuun listattu muutamia osapuolten käytössä olevia ja saatavilla olevia valmiita malleja käyttäjähallinnan alueella. Malleja on myös soveltuvin osin suhteutettu edellisissä luvuissa kuvattuihin palveluihin ja toimintoihin.

- TUPAS-palvelut (asiakkaan tunnistuspalvelu ja sessionhallintapalvelu) (FK 2008)
- Minimikontekstinhallinnan määrittelyt (sessionhallintapalvelu, kontekstipalvelu, kertakirjautumispalvelu)
- Ydinpalvelurajapinnat-liittymämäärittelyt: AuthorizationAccess (pääsynvalvontapalvelu), AuthenticateUser (tunnistuspalvelu, sessionhallintapalvelu) sekä User:ProfileAccess (käyttäjäprofiilipalvelu) (Sormunen ym. 2005)
- OMG:n Resource Access Decision -palveluäärittelyt (pääsynvalvontapalvelu)
- SAML ID Provider ja Security Token Service (tunnistuspalvelu ja käyttäjäprofiilipalvelu) (Hughes ym. 2004)
- OpenID-malli (hajautettu tunnistuspalvelu, käyttäjäprofiilipalvelu) (Smarr 2007)
- WS-Trust-, WS-SecureConversation- (sessionhallinta- ja tunnistuspalvelut), WS-Federation- (federointipalvelut), WS-Policy- ja WS-SecurityPolicy (pääsynvalvontapiste, pääsynvalvontapalvelu, roolipalvelut, käyttäjäprofiilipalvelut) -suositukset (Sormunen ym. 2007)
- Liberty Alliancen määritykset: IAF-Identity Assurance Framework (federointipalvelut, käyttäjäprofiilipalvelut) ja IGF - Identity Governance Framework (käyttäjä- ja pääsynhallinta ja provisiointi) (Landau ym. 2003)
- ISO/TS 22600-2:2006 (ISO 22600:2) standardi sisältää arkkitehtuurikomponenttien malleja valtuuksien ja pääsynhallintaan: Domain Model, Document Model, Policy Model, Role Model, Authorization Model, Delegation Model, Control Model ja Access Control Model.
- IHE:n aihealueeseen liittyviä määrityksiä ovat mm. XUA - Cross-Enterprise User Assertion (federointipalvelut, roolipalvelut), EUA - Enterprise User Authentication (käyttäjätunnusten yhtenäistäminen, käyttäjätunnistus), ATNA - Audit Trail and Node Authentication (käyttövaltuuksien tarkistukset, järjestelmien tunnistaminen), PWP - Personnel White Pages (käyttäjähakemisto, käyttäjäprofiilipalvelu), BPPC - Basic Patient Privacy Consents (kontekstipalvelut / suostumus) (IHE 2007)
- HSSP PASS (Privacy, Authentication and Security Services) -palvelut: Audit service (lokipalvelut) ja Access Control Services
- lukuisa määrä IdM- ja IAM-tuotteiden tarjoamia valmiita malleja ja rajapintoja (sisältävät usein etenkin käyttäjä- ja roolihallinnan sekä kertakirjautumisen tai tunnusten sekä käyttäjätietojen välityksen ja provisioinnin sekä monia käyttäjä-, rooli- ja oikeushallinnan työnkulkuja)
- VAHTI-suositukset (VAHTI 2006) sekä TJSert-hankkeen vaatimukset suostumuksiin, käyttäjien tunnistamiseen ja pääsynvalvontaan (Ruotsalainen ym. 2008).

# 10 Yhteenveto

Tähän dokumenttiin on koottu käyttäjä- ja käytönhallinnan malleja, joita on tutkittu ja kehitetty SOLEA-hankkeen työpajoissa yhteistyössä projektiin osallistuneiden organisaatioiden kanssa. Dokumentin sisältämien mallien avulla on useissaeri työpajoissa ja kuvatussa case-esimerkissä jäsennetty käyttäjä- ja käytönhallinnan kohdealuetta. Esitetyt mallit ja jäsennykset ovat yleiskäyttöisiä ja niitä voidaan käyttää pohjana organisaatiokohtaisille tarkennuksille. Kehittämisen kohteeksi on mahdollista valita vain osa kuvatuista osa-alueista. Dokumentin prosesseja, toimintoja ja tehtäviä on käytetty esimerkkinä myös SOLEA-hankkeen prosessien ja toiminnan kuvaamisen tutkimus- ja kehitystyössä.

Dokumentin jatkohyödyntämisessä on mahdollisuus esimerkiksi organisaatiokohtaisesti:

- tuottaa palvelukuvaustaulukoita myös muista tunnistetuista tarpeellisiksi nähdyistä palveluista,
- tarkentaa palvelujen välistä arkkitehtuuria tarkempien rajapintojen, kutsusuhteiden sekä tietoarkkitehtuurin osalta, pohjautuen konkreettisiin tarpeisiin,
- arvioida eri palveluihin ja niiden välisiin suhteisiin soveltuvia valmiita malleja (luvun 9 pohjalta) ja tuotetoteutuksia.
- tarkentaa, mitä palveluja tai arkkitehtuurimalleja tullaan määrittelemään tarkemmin.

Käytetyt jäsennykset ovat esimerkki toiminta- ja palvelulähtöisestä kohdealueen kuvaamisesta, joka on mahdollista sovittaa kokonaisarkkitehtuurimenetelmiin ja -jäsennyksiin. Mukana on myös esimerkki kohdealueen kehittämistavoitteiden kuvaamisesta mittarien kautta. Palvelu- ja toimintokeskeisyys luo pohjaa hyödyntää tuotoksia joustavasti suuremmissa tai pienemmissä kokonaisuuksissa. Vaikka tietojärjestelmäratkaisujen kuvaaminen painottuukin SOA-tyyppiseen jäsentämiseen, on vastaavia palveluita mahdollista tunnistaa ja toteuttaa erityyppisillä järjestelmä- ja teknologiaratkaisuilla eri tavoin jäsenneltynä.

# Lähteet


| |
|---|
| FK 2008. Palvelukuvaukset: Tietoturva ja asiakasyhteydet / Tupas-varmennepalvelu. Finanssialan keskusliitto, 2008. http://www.fkl.fi/asp/system/empty.asp?P=2414&VID=default&SID=756755896942990&S=1&C=24989 |
| Hughes J et al. Technical Overview of the OASIS Security Assertion Markup Language (SAML) V1.1. OASIS, May 2004. |
| IHE 2007. HIE Security and Privacy through IHE. IHE IT Infrastructure White Paper, Integrating the Healthcare Enterprise, draft, ACC/HIMSS/RSNA, 2007. |
| ISO 22600:2. Health informatics - Privilege management and access control Formal models. ISO Technical Standard ISO/TS 22600 2:2006. |
| JHS 179: http://www.jhs-suositukset.fi/suomi/jhs179, JUHTA-julkisen hallinon tietohallinnon neuvottelukunta, 2011. |
| Landau S, ed. Liberty ID-WSF Security and Privacy Overview. Liberty Alliance Project, 2003. |
| Luukkonen I, Mykkänen J, Itälä T, Savolainen S, Tamminen M. Toiminnan ja prosessien mallintaminen - tasot, näkökulmat ja esimerkit. SOLEA-hanke, Itä-Suomen yliopisto, Aalto-yliopisto, 2012. |
| Ruotsalainen P, Kaskinen T, Mykkänen J. Terveydenhuollon tietojärjestelmien sertifiointivaatimukset; Osa 2 vaatimukset potilasasiakirjoja käsitteleville tietojärjestelmille, KANTA- palvelulle ja viestinnän osapuolille. TJSERT-hanke, Stakes, 2008. |
| Smarr J. A recipe for OpenID-Enabling Your Site. Plaxo Inc., 2007. http://www.plaxo.com/api/openid_recipe |
| Sormunen M, Jäntti M, Rannanheimo J, Mykkänen J. Ydinpalvelurajapinnat (käyttäjä, käyttöoikeus, potilas): Tekninen liittymämäärittely http- ja XML-tekniikoilla. Versio 2.1. HL7 Finland, 2005. http://virtual.vtt.fi/virtual/hl7/cda/api-rajapinnat/120505ydinpalvelurajapinnat-v21.doc |
| Sormunen M, Mykkänen J, Luostarinen H, Saesmaa M. Web-sovelluspalvelujen tekniset määritykset. SerAPI-projekti, Kuopion yliopisto, 2007. |
| VAHTI 2006. Käyttövaltuushallinnon periaatteet ja hyvät käytännöt. Valtionhallinnon tietoturvallisuuden johtoryhmä, VM, VAHTI 9/2006. |
| VAHTI 2008. Lokiohje. Valtionhallinnon tietoturvallisuuden johtoryhmä, VM, Luonnos 9.9.2008. |
| Virkanen H, Järvinen J, Mykkänen J, Sammelvuo I. Arkkitehtuurikuvausten kohteet ja kuvaustavat - kooste case-tutkimuksen tuloksista. SOLEA-hanke, Itä-Suomen yliopisto, Aalto-yliopisto, 2012. |
| VIRTU-käyttäjähallintokoulu-materiaali, Valtiovarainministeriö, 2008. |

# Liite 1. Case-kuvaus: Istekki/PSshp, menetelmien ja välineiden hyödyntäminen

Seuraava luvussa esitetään tässä dokumentissa esiteltyjen menetelmien ja välineiden hyödyntämistä sekä soveltamista hankkeen osapuolella meneillään olevassa käyttäjähallinnan kehittämishankkeessa. Tässä dokumentissa estettyjen menetelmien (Liite 1, luku 2 ja sen aliluvut) ohella kyseisessä case-kohteessa hyödynnettiin ja sovellettiin myös toisen SOLEA-kohteen tuotoksia: *Arkkitehtuurin kuvaustapojen case-tiedonkeruulomakkeet* (Virkanen ym. 2012, Liite 1, luku 3 ja sen aliluvut).

Seuraavissa aliluvuissa kuvataan kehittämishankkeelle suoritettu läpikäynti menetelmittäin. Menetelmäkohtaisissa luvuissa käydään läpi seuraavat pääkohdat:

- menetelmä tai väline
- tapa, jolla menetelmää hyödynnettiin
- menetelmällä tai välineellä saavutetut tulokset
- sekä arviointia ja näkemyksiä tapauskohtaisesti (esiin nousseita havaintoja, joko tutkijoiden tai aihealueen asiantuntijan toimesta, mm. jatkokehitysideoita ja tarkennuksia)

Läpikäynnissä tarkasteluta suoritettiin lähinnä ratkaisun tavoitetilan suhteen ja nykytilasta kirjattiin ylös periaatetason ratkaisut, mallit ja toimintatavat, jotka hyödynnettävissä myös tulevassa kokonaisratkaisussa. Läpikäynnin tarkoituksen oli tuottaa molemmille osallistuville osapuolille (tutkijat ja haastateltavat) hyötyjä, mm. seuraavasti:

- haastateltavan vetämän projektin läpikäynti tutkimushankkeessa tuotetuin usein eri menetelmin, pääasiassa tarkastuslista tyyppisesti, tuotti alkuvaiheessa olevalle projektille sisältöjen ja suunniteltujen kokonaisuuksien suhteen täydennystä (mm. tarvittavien kuvausten) sekä työkohteille useita alustavia priorisointi-/vaiheistuslistauksia
- tutkimusosapuolelle tuotettujen mallien hyödyntäminen käytännön projektin yhteydessä auttoi mm. menetelmien ja välineiden järkevyys-/kattavuustarkastelussa, täydentämään välineitä sekä kehittämään välineistön hyödyntämismalleja

Edellä mainitut seikat pyritty kirjaamaan varsinaisten määrityskohteeseen liittyvien havaintojen oheen tässä case-osiossa. Menetelmillä saatujen ratkaisujen oheen on haettu, lähinnä tavoitetilan kuvasten ja läpikäyntien tuloksien jatko hyödyntämistä silmälläpitäen JHS 179-mallin (Itälä ym. 2012) kuvauspohjia ja niiden soveltamisohjeita menetelmittäin. Tarkoituksena esittää ja selventää kokonaisarkkitehtuurimenetelmien soveltuvuutta kohdealueen kartoittamiseen sekä myös niiden hyödyntämistä SOLEA- mallien ja välineiden ohessa.

Läpikäynnit suoritettiin yhteensä neljässä 2-4 tunnin työpajaluontoisessa tapaamisessa (aikavälillä: 3-6/2011), vaihtelevalla kokoonpanolla tutkijoiden (1-2hloä/tapaaminen) ja organisaation aihealueen asiantuntijoiden (1-2hlöä/tapaaminen) kesken. Läpikäynti suoritettiin ennakkoon jaetun materiaalin (menetelmät ja lomakkeet) pohjalta, tutkijoiden pääasiallisesti haastatellessa asiantuntijoita ja johtaessa keskustelua, samalla kirjaten havaintoja ja tuloksia, niin tutkimusryhmä kuin asiantuntijapuolen käyttöön ja hyödynnettäväksi omissa dokumentaatioissa. Tutkimusryhmä sai myös taustoitukseksi luettavakseen hankkeen sen hetkisen projektidokumentaation (lähinnä projektisuunnitelmia ja projektin organisoitumista koskevaa materiaalia). Organisaation pääasiantuntija on kyseisen vielä kartoitus-/selvitysvaiheessa olevan hankeen vetäjä ja töissä ratkaisun toimittajalla (Istekki). Toinen

osallistuja toimii ratkaisun tilaavan/hankkivan organisaation (KYS/Pohjois-Savon sairaanhoitopiiri) tietohallinnossa kehittämispäällikkönä.

# 1. Taustaa

Yhteistyö SOLEA-hankkeen sekä ratkaisun hankkijan välillä on suoritettu kahdessa eri jaksossa, ensimmäisellä kertaa tilaajan hankinta-/määritysprojekti lykkääntyi mm. henkilöstö- ja organisaatiomuutosten johdosta case-kohteena olleessa organisaatiossa. Ensimmäisellä läpikäyntikierroksella (2008-2009) hyödynnettiin silloista työversiota SOLEA-dokumentista: *Vaatimukset ja rajaukset palvelupohjaiselle käyttäjä- ja käytönhallinnalle*, joka sisälsi jo tuolloin pääasiallisesti samat menetelmät ja välineet ja niitä hyödynnettiin käytettiin esikartoitusvaiheessa hankkeen silloisten tekijöiden toimesta. Tuolloin aikaansaatua organisaation sisäistä kartoitusdokumentaatiota on hyödynnetty myös hankkeen jatkossa (seuraavalla kierroksella) tausta- ja pohjamateriaalina.

Uudelleen käynnistetyn selvityshankkeen tarkoituksena on: *”Selvitysprojektissa Istekki Oy (jatkossa Istekki) selvittää Pohjois-Savon sairaanhoitopiirin (jatkossa shp) käyttäjähallinnan vaateet, roolit ja käyttäjähallintaan liittyvät prosessit. Hankkeessa tehdään myös käyttäjähallinta-tuotteen hankinta ja suunnitellaan vaiheistetut toteutus- ja käyttöönotto-projektit”*.

lainaus: Istekkin IdM- käyttäjähallinnan selvitysprojektidokumentaatiosta 10.1.2011

Tarkentavia tavoitteita sekä rajauksia nousi läpikäyntien yhteydessä esiin ja niitä on myös kirjattu mukaan läpikäynnin tuloksiin menetelmäkohtaisesti seuraavissa aliluvuissa. Esiin nousseita ja läpikäyntien aikana saatuja tarkennuksia, linjauksia ja rajauksia on jo hyödynnetty ja tullaan jatkossa hyödyntämään myös itse hankkeen dokumentaatiossa. Samoin kuin itse SOLEA:n aihealueelle tässä dokumentissa kirjattua näkemystä kohdealueesta mm. käsitteistö nähtiin hyödynnettäväksi sellaisenaan.

# 2 Vaatimukset ja rajaukset palvelupohjaiselle käyttäjä- ja käytönhallinnalle-dokumentin välineet ja menetelmät

## 2.1 Kehittämistarpeet ja niistä saaduille hyödyille asetetut mittarit

**Menetelmä tai väline:**

ks. tarkemmin dokumentin luku: *3 Käyttäjähallinta - yhteisiä kehittämistarpeita*

| **Kehittämistarve** | **Mittarit** |
|---|---|
| Käyttäjähallinnan yhdistäminen henkilöstöhallinnon prosesseihin. | Henkilöstöhallinnon lisäksi muualla tarvittavien käyttäjähallinnan toimenpiteiden työmäärä.<br>Erillisten käyttäjähallintaan liittyvien (henkilöille kohdistuvien) palvelupyyntöjen määrä. |
| Käyttäjien tunnistaminen ja todentaminen yhdenmukaisesti. | Erilaisten tunnistamis- ja todentamistapojen lukumäärän väheneminen<br>Yhdenmukaisten tunnistamis- ja todentamispalvelujen käyttöaste (kuinka suuri osuus sovelluksista tai tunnistustapahtumista käyttää yhdenmukaisia palveluja) |
| Käytäntöjen yhtenäistäminen eri sovelluksissa liittyen käyttäjien ja käytön hallintaan | Yhtenäisiä käyttäjähallinta-, tunnistus- ja pääsynvalvontaratkaisuja käyttävien sovellusten tai käyttötilanteiden osuus kaikista. Yhden käyttäjän käyttäjätilien lukumäärä. Ylläpitotyön määrä ja kustannukset käyttäjätunnusten tekoon. Käyttövaltuuksien saannin ja käsittelyn odottamiseen kuluva aika. |
| Käyttäjätietojen yhdistäminen henkilöiden työrooleihin ja staattisiin käyttöoikeuksiin | Käyttöoikeuksien määrittelyt on sidottu rooleihin. Käyttäjien määrittely voidaan tehdä erillään työroolien määrittelyistä. (RBAC, role-based access control). |
| Käyttäjähallinnan yhdistäminen dynaamisiin, vuorovaikutussuhteista tai muista henkilöistä riippuviin käyttöoikeuksiin (esim. asiayhteyden päättely terveydenhuollossa) | Tarkastus: voidaanko käyttövaltuuksien tarkastamisen yhteydessä huomioida tarvittavia dynaamisia vuorovaikutussuhteita. |
| Kertakirjautuminen (SSO) | Käyttäjän kirjautumistoimenpiteiden lukumäärä / ajanjakso. Käyttäjän käyttäjätunnusten tai käyttäjätunnus / salasanaparien lukumäärä. Kirjautumistoimenpiteisiin käytetty aika / ajanjakso. Kirjautumistransaktion hinta. |
| Vahvan tunnistamisen käyttöönotto, ulkoisten varmennepalvelujen tai toimikorttien käyttöönotto | Ratkaisujen kautta hoidettava osuus tunnistustapahtumista. Ko. ratkaisuilla hoidettavien tunnistamistapahtumien lukumäärä. Ratkaisujen piirissä olevien sovellusten lukumäärä ja osuus kaikista sovelluksista. |
| Organisaation ulkopuolisten käyttäjien huomiointi käyttäjähallintaratkaisuissa. | Esimerkiksi federoidun käyttäjähallintaratkaisun (ml. toimintatavat) käyttöönoton onnistuminen. |

| | |
|---|---|
| | Ks. myös edellinen rivi. |

**Menetelmän tai välineen hyödyntäminen**

Alustukseksi käyty menetelmän selvittäminen osallistujille, jonka jälkeen keskustelu: kehittämistarpeista ja niille asetettavista mittareista.

**Menetelmällä tai välineellä saavutetut tulokset:**

Todettiin, että kartoitusvaiheessa on vielä liian aikaista ryhtyä asettamaan kehittämistarpeille mittareita, mutta useat listauksessa olevat kehitystarpeet ovat jo mukana projektissa (mm. SSO, toimikorttien käyttöönotto, organisaation ulkopuoliset käyttäjät ja roolit). Tulokseksi lähinnä haastateltavan arvio tai suunnitelma menetelmän hyödyntämisestä ja sen koekäytöstä, esim. seuraavalla tavalla: priorisoidaan taulukon Kehittämistarpeista viisi tärkeintä, joille tehtäisiin tarkentaminen niille asetettavien mittareiden suhteen.

**Arviointi ja näkemykset**

Ei näkemystä menetelmälle vielä projektin alustavassa vaiheissa, mutta jo itse kehitystarpeiden lista hyödynnettävissä sinällään tekemisen priorisoinnissa. Sen sijaan tarkkojen mittareiden asettaminen kartoituksessa nähtiin vielä liian aikaiseksi projektin kannalta.

SOLEAssa tuotetussa Kehittämistarpeita ja niille asetettavia mittareita mallin läpikäynnissä ja saatujen tulosten kirjaamisessa ja edelleen tarkentamisessa hyödynnettävissä JHS 179 –mallista löytyvät kaksi taulukkoa: *Kehittämisvaatimukset ja tavoitteet* sekä *Sidosryhmien vaatimukset ja tavoitteet*, joissa yhdistetty vastaavaan tapaan kuin SOLEA-mallissa kohdealueelle asetetut kehittämistarpeet (JHS-vaatimukset) ja niille asetettava mittarit. Tarkemmin kehitystarpeista ja vaatimuksista seuraavassa aliluvussa.

Kehittämisvaatimukset ja tavoitteet

Päiväys

Versio

Prioriteetti: 1=välttämätön, 2=hyödyllinen, 3= toivottu

Tyyppi= toiminnallinen, luotettavuus, käytettävyys, tehokkuus, ylläpidettävyys, siirrettävyys, tietoturvallisuus

| Vaatimuksen/ kehitystarpeen kuvaus | Vaatimuksen alkuperä/ esittäjä | Päivä | Hyötynäkökulma | Vaatimuksen tyyppi | Edellytys | Tavoitetila | Mittari | Organisaation tavoitearvo | Tila | Prioriteetti |
|---|---|---|---|---|---|---|---|---|---|---|
| <Vaatimus1> | | | | | | | Mittari vaatimukselle 1 | Mittarin tavoitearvo | | |
| <Vaatimus 2> | | | | | | | | | | |
| <Vaatimus 3> | | | | | | | | | | |
| <Vaatimus 4> | | | | | | | | | | |

**Kuva 1**: JHS 179 Kehittämisvaatimukset ja tavoitteet –taulukko.

Sidosryhmien vaatimukset ja tavoitteet -taulukko

Päiväys

Versio

Prioriteetti: 1=välttämätön, 2=hyödyllinen, 3= toivottu

Tyyppi= toiminnallinen, luotettavuus, käytettävyys, tehokkuus, ylläpidettävyys, siirrettävyys

| Sidosryhmä | Vaatimus | Päivä | Vaatimuksen tyyppi | Edellytys | Mittari | Organisaation tavoitearvo | Tila | Prioriteetti |
|---|---|---|---|---|---|---|---|---|
| <Sidosryhmä1> | | | | | | | | |
| | <Vaatimus 1> | | | | Mittari vaatimukselle 1 | Vaatimuksen 1 mittarin tavoitearvo | | |
| | <Vaatimus 2> | | | | | | | |
| <Sidosryhmä 2> | | | | | | | | |
| | <Vaatimus 3> | | | | | | | |

**Kuva 2**: JHS 179 Sidosryhmien vaatimukset ja tavoitteet –taulukko.

## 2.2 Kohdealueen jäsentämismalli

### Menetelmä tai väline:

ks. tarkemmin dokumentin luku: *4 Käyttäjähallinnan jäsentämismalli* (myös alla)

| | organisaation hallinnoimat käyttäjät / työntekijät | asiakas- tai kansalaiskäyttäjät | kumppaniorganisaatioiden hallinnoimat käyttäjät (luottamusverkosto) |
|---|---|---|---|
| käyttäjien, roolien ja valtuuksien määrittely | | | |
| käyttäjien tunnistaminen ja todentaminen | | | |
| pääsynvalvonta | | | |
| käytön seuranta | | | |

### Menetelmän tai välineen hyödyntäminen

Alustukseksi menetelmän selvittäminen osallistujille jonka jälkeen keskustelu: Mitkä eri jäsennysmallin kentistä (osa-alueista) kuuluvat hahmotellun ratkaisun piiriin? Keskustelun tulokset kirjattiin taulukkoon.

**Menetelmällä tai välineellä saavutetut tulokset:**

| | organisaation hallinnoimat käyttäjät / työntekijät | asiakas- tai kansalaiskäyttäjät | kumppaniorganisaatioiden hallinnoimat käyttäjät (luottamusverkosto) |
|---|---|---|---|
| käyttäjien, roolien ja valtuuksien määrittely | X | | (X) |
| käyttäjien tunnistaminen ja todentaminen | X | | (X) |
| pääsynvalvonta | (X) / osittain -enemmän kohti keskitettyä autorisointia (keskitetty hakemistopalvelu), muttei juurikaan ulkoistettavissa järjestelmistä | | (-keskitetty hakemistopalvelu) |
| käytön seuranta | (X) / hyvin vähän – maksimi: IDM:n historiatiedot pääsyvaltuuksista/oikeuksista, toisaalla/välillisesti mm. luovutusten seuranta valtakunnallisesti KanTassa | | (X) / hyvin vähän – maksimi: IDM:n historiatiedot pääsyvaltuuksista/oikeuksista, toisaalla/välillisesti mm. luovutusten seuranta valtakunnallisesti KanTassa |

Läpikäynnillä ja keskustelulla tunnistettiin projektin pääpainopiste (rastit taulukon soluissa) eri käyttäjätyyppien (sarakeotsikot) ja kyseiselle käyttäjätyypille yhdenmukaisesti toteutettavaan toiminnallisuuden (riviotsikot) suhteen. Samalla myös saatiin aikaan näkemys projektin mahdollisesta vaiheistuksesta ts. suluissa olevat rastit taulukon soluissa tulevat mahdollisesti tarkennettaviksi ja toteutettaviksi jatkossa. Tarvittaessa soluihin kirjattiin tarkennuksia ja rajauksia työkohteiden suhteen (vapaa teksti kentissä).

Projekti keskittyy varsinaisesti kohdealueella seuraaviin päätoimintoihin: *Käyttäjien, roolien ja valtuuksien määrittelyyn* sekä *Käyttäjien tunnistaminen ja todentamiseen* ja lähinnä näiden osa-alueiden keskittämiseen organisaation hallinnoimien käyttäjien suhteen (ts. omat työntekijät). Pääsynvalvontapuolella tekemisen rajaamisessa esim. seuraavanlainen linjanvedon tekeminen näytti todennäköiseltä: ”*projektissa keskitytty pääsynhallintaan vaan järjestelmätasolla, ja järjestelmät hoitavat pääsynvalvonnan tietokohtaisesti*”.

**Arviointi ja näkemykset**

Läpikäynnissä tunnistettiin kyseisen projektin ja organisaation osalta vielä yksi käyttäjätyyppi, jonka osalta nähtiin hyödylliseksi täydentää annettua kehikkoa (sarake merkattu alla olevassa taulukossa sinisellä). Kyseisessä sarakkeessa ilmenevä ”uusi” käyttäjätyyppi edustaa organisaatiossa poikkeustapauksia, jotka tarvitsevat lähinnä lyhytaikaista tai/sekä tilapäistä pääsyä organisaation hallitsemiin tietojärjestelmiin ja palveluihin vaihtelevilla oikeuksilla. Tällaisia käyttäjiä ovat tyypillisesti opiskelijat, tietojärjestelmätoimittajat ja erityyppiset asiantuntijat sekä ostopalveluiden kautta organisaation järjestelmiin pääsyä tarvitseva henkilöstö.

Samalla keskustelussa nousi esiin karkea vaiheistus ja myös rajaus projektille eli ratkaisuja ryhdytään totuttamaan eri käyttäjätyypeille eri vaiheissa sekä yksi käyttäjätyhmä tuli rajatuksi tämän ratkaisun ulkopuolelle.

| | organisaation hallinnoimat käyttäjät / työntekijät | asiakas- tai kansalaiskäyttäjät | kumppaniorganisaatioiden hallinnoimat käyttäjät (luottamusverkosto) | tilapäistyöntekijät (ostopalvelut), opiskelijat, järjestelmätoimittajat, konsultit |
|---|---|---|---|---|
| käyttäjien, roolien ja valtuuksien määrittely | | | | |
| käyttäjien tunnistaminen ja todentaminen | | | | |
| pääsynvalvonta | | | | |
| käytön seuranta | | | | |

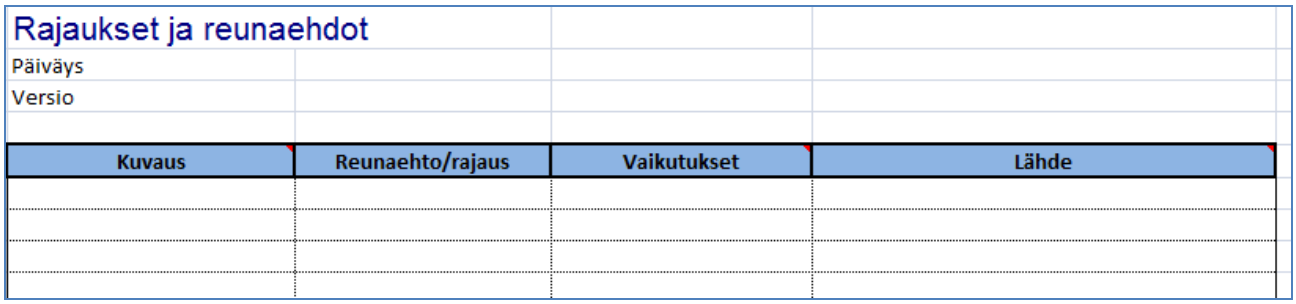
***Yhteenveto välineellä saavutetuista tuloksista:***
- linjauksia
- rajauksia
- vaiheistusta
- työpakettipohjia
- käyttäjätyyppien tunnistaminen

Kaikki edellä listatut tuotokset saatu aikaan lähinnä vasta karkealla tasolla ja niitä on tarkennettava jatkossa, esim. läpikäynnissä jatkossa hyödynnettävillä välineillä, kuten toiminnallisuuksien tarkennuksiin on mentävissä tässä dokumentaatiossa esiteltävän seuraava välineen avulla: *Kohdealueen perusprosessit ja toiminnot –tarkastuslista*. Samalla havaittu, että valmiit listaukset SOLEA-malleissa voivat toimia tarkistuslistoina ja/myös vain ehdotuksina tai mallitemplaatteina, siitä mitä ratkaisukenttä sisältää. Esimerkkinä tästä tunnistettu, mallin ulkopuoleinen käyttäjätyyppi, jonka lisääminen ehdotettuun malliin on tehty kyseisen hankkeen ratkaisumallin kartoittamista varten. Ts. nähty oleellisena myös tarkastella tämän menetelmän mallin yhteydessä (ja myös muiden mallilistauksien ohella), jääkö jotain ehdotetun mallin ulkopuolelle. tyypillisesti tällaisia arvoja ovat eri poikkeustapaukset, joille ei välttämättä saada rakennettua yhdenmukaista ratkaisumallia.

Jatkotoimenpiteinä tämän menetelmän käytölle nähtiin edellä mainittu toiminnallisuuksien tarkentaminen: *Kohdealueen perusprosessit ja toiminnot –tarkastuslistaa* hyödyntäen. Saatujen ratkaisujen ja päätösten ylöskirjaamiseen on hyödynnettävissä välineen ohessa mm. seuraavien SOLEA-hankkeessa tarkemmin tarkasteltujen mallien JHS 179 valmiita kuvauspohjia (tarkemmin kuvissa alla, nämä tunnistettu tutkimuksen tekijöiden osalta jälkikäteen arviointia suoritettaessa):

***1) Linjauksien, rajauksien, vaiheistuksen kirjaaminen***

Seuraavissa kuvissa esitellyissä taulukoissa saatujen rajauksien, linjauksien ja vaiheistuksen (sekä alustavaa työpakettijakoa: useimmat vaatimukset yms. aiheuttanevat loppujen lopuksi omia työ-/toteutuskokonaisuuksia) kirjaaminen hyödynnettävissä oleviin valmiisiin kuvauspohjiin.



Rajaukset ja reunaehdot

Päiväys

Versio

| Kuvaus | Reunaehto/rajaus | Vaikutukset | Lähde |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

**Kuva 3**: Saatujen rajauksien kirjaamiseen hyödynnettävissä oleva JHS 179 Rajaukset ja reunaehdot –taulukko.

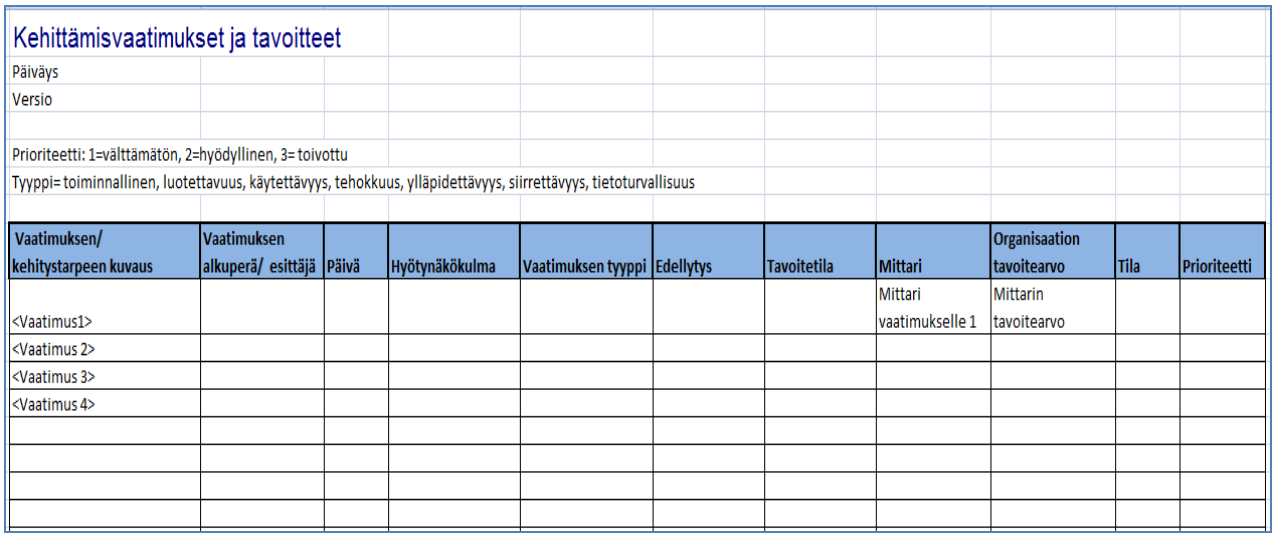
Arkkitehtuuriperiaatteet

Päiväys

Versio

| Nimi | Kuvaus | Perustelu | Seuraukset | Periaatteen lähde |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**Kuva 4**: Tuotetut linjaukset ovat jalostettavissa esim. arkkitehtuuriperiaatteiksi - JHS 179 *Arkkitehtuuriperiaatteet* –taulukko (vasemmalla).



Kehittämisvaatimukset ja tavoitteet

Päiväys

Versio

Prioriteetti: 1=välttämätön, 2=hyödyllinen, 3= toivottu

Tyyppi= toiminnallinen, luotettavuus, käytettävyys, tehokkuus, ylläpidettävyys, siirrettävyys, tietoturvallisuus

| Vaatimuksen/ kehitystarpeen kuvaus | Vaatimuksen alkuperä/ esittäjä | Päivä | Hyötynäkökulma | Vaatimuksen tyyppi | Edellytys | Tavoitetila | Mittari | Organisaation tavoitearvo | Tila | Prioriteetti |
|---|---|---|---|---|---|---|---|---|---|---|
| <Vaatimus1> | | | | | | | Mittari vaatimukselle 1 | Mittarin tavoitearvo | | |
| <Vaatimus 2> | | | | | | | | | | |
| <Vaatimus 3> | | | | | | | | | | |
| <Vaatimus 4> | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

**Kuva 5:** Tuotetut linjaukset tarkennettavissa myös JHS 179 *Kehittämisvaatimukset ja tavoitteet* –taulukossa vaatimuksiksi (HUOM: mukaan kirjattavissa myös läpikäynnin aikana saadut vaiheistukseen ja tärkeysjärjestykseen liittyvät näkemykset, sarake: *Prioriteetti*, arvoavaruus: *1=välttämätön, 2=hyödyllinen, 3= toivottu*)

### *2) Käyttäjätyyppien tunnistaminen - tulosten kirjaaminen*

Vastaavasti myös JHS 179 Sidosryhmät - sekä Organisaatiot ja sidosryhmät –kuvausten kautta on avattavissa käyttäjien roolien ja valtuutuksien määrittelytyötä (karkea rajaus rooleihin ja organisaatioihin jo itse SOLEA-mallin käyttäjätyypeissä).

Sidosryhmät

Päiväys

Versio

| Sidosryhmä | Kuvaus | Sidosryhmän rooli | Sidosryhmän tehtävät ja vastuut | Sidosryhmän saamat palvelut/tuotokset | Sähköisen asioinnin toimija | Muuta |
|---|---|---|---|---|---|---|
| Sidosryhmätyyppi | | | | | | |
| <Sidosryhmä> | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

**Kuva 6:** JHS 179 *Sidosryhmät* -taulukko.

Organisaatiot ja sidosryhmät

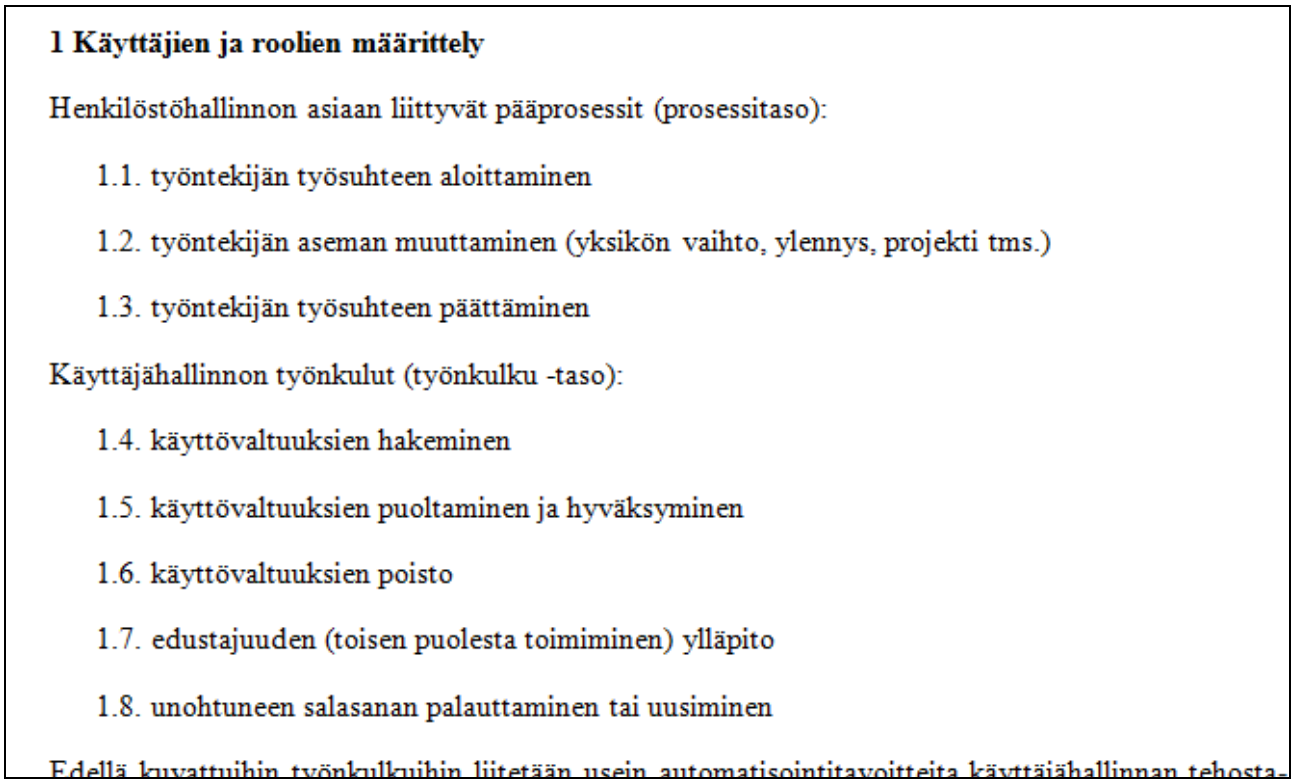
| Organisaatio tai sidosryhmä (Toimija) | Tärkeys | Kuvaus | Vastuu/oikeus | Henkilö lkm |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Muut | | | | |
| | | | | |
| | | | | |
| | | | | |

**Kuva 7**: JHS 179 *Organisaatiot ja sidosryhmät* –matriisi.

## 2.3 Kohdealueen perusprosessit ja toiminnot –tarkastuslista

**Menetelmä tai väline**

ks. dokumentin luku: *5 Käyttäjähallinnan perusprosessit ja toiminnot*



**1 Käyttäjien ja roolien määrittely**

Henkilöstöhallinnon asiaan liittyvät pääprosessit (prosessitaso):

1.1. työntekijän työsuhteen aloittaminen

1.2. työntekijän aseman muuttaminen (yksikön vaihto, ylennys, projekti tms.)

1.3. työntekijän työsuhteen päättäminen

Käyttäjähallinnon työnkulut (työnkulku -taso):

1.4. käyttövaltuuksien hakeminen

1.5. käyttövaltuuksien puoltaminen ja hyväksyminen

1.6. käyttövaltuuksien poisto

1.7. edustajuuden (toisen puolesta toimiminen) ylläpito

1.8. unohtuneen salasanan palauttaminen tai uusiminen

Edellä kuvattuihin työnkulkuihin liitetään usein automatisointitavoitteita käyttäjähallinnan tehosta-

**Kuva 8**: Esimerkkiotos käyttäjähallinnan perusprosessit ja –toiminnot -listauksesta

**Menetelmän tai välineen hyödyntäminen**

Alustukseksi menetelmän selvittäminen osallistujille, jonka jälkeen keskustelu: Mitkä eri listatuista prosesseista ja toiminnoista, kuuluvat hahmotellun ratkaisun piiriin? Keskustelun tulokset, niin toteutettaviksi valitut prosessit ja työnkulut kuin näihin liittyvät havainnot ja tarkennukset kirjattiin dokumenttipohjaan.

Prosessi- ja työnkulkuryhmien karsimisessa voidaan käyttää edellisessä luvussa hyödynnetyn mallin (*Kohdealueen jäsentämismalli*) avulla tuotettuja rajauksia työn nopeuttamiseksi, mutta toisaalta esim. työlistoilta jo poissuljettujen osien, vaikka kursorinen, läpikäynti voi auttaa vahvistamaan tai johtaa korjaamaan, edellisessä vaiheessa tehtyjä rajauksia.

**Menetelmällä tai välineellä saavutetut tulokset**

**1 Käyttäjien ja roolien määrittely**

1.1. työntekijän työsuhteen aloittaminen- KYLLÄ:

tarkentuu kolmeksi alakohdaksi (alkupisteeksi) nykytilassa/ei vielä parannusehdotuksia tullut – kaikki tulevat kuitenkin töihin yhden pisteen kautta

- työpalvelun kautta
- yksikön kautta (vakituinen/lääkärit/...)
- keikkalainen: rekryksi

1.2. työntekijän aseman muuttaminen (yksikön vaihto, ylennys, projekti tms.) KYLLÄ

- nykyinen paperinen käytäntö - aseman muutos: erokirja/uusi sopimus seuraavaan positioon: korjattavaa/viiltattavaa/prosessin sujuvoittamista, mm. provisiointi

1.3. työntekijän työsuhteen päättäminen nykytila KYLLÄ/tavoitetila

- yksiköltä ilmoitus työsuhteen päättämisestä ja 2. krt vuoteen ajetaan läpi tarkastukset
- henkilöstöhallinnonjärjestelmä ei voi toimia kaikissa masterina (70% menee tätä kautta), poikkeukset otettava huomioon kuitenkin aina

Käyttäjähallinnon työnkulut (työnkulku -taso):

1.4. käyttövaltuuksien hakeminen KYLLÄ

- nykytilassa lomakkeiden kautta

1.5. käyttövaltuuksien nuoltaminen ja hyväksyminen KYLLÄ

**Kuva 9**: Esimerkki käyttäjähallinnan perusprosessit ja –toiminnot –listauksesta ja sen oheen haastattelijan tekemät merkinnät (sinisellä alleviivattuina).

Listauksen läpikäynnin tulokset heijastelivat samaa linjausta, mikä ilmenee myös *Kohdealueen jäsentämismallin* (Liite 1, luku 2.2) hyödyntämisessä: projekti keskittyy kohdealueella pääasiallisesti kahteen osa-alueeseen: *Käyttäjien, roolien ja valtuuksien määrittelyyn* ja *Käyttäjien tunnistaminen ja todentamiseen.* Ts. näiden kahden osa-alueen kaikki listatut prosessit ja toiminnot nähtiin toteuttamiskelpoisiksi ja niitä tullaan toteuttamaan tai edelleen kehittämään tulevassa ratkaisumallissa.

**Arviointi ja näkemykset**

Mallilla saadaan edelleen tarkennettua, vahvistettu tai uudelleenlinjattua jos aiemmissa vaiheissa tehtyjä toiminnallisuuden suhteen tehtyjä valintoja.

Nähtävissä on, että kyseinen malli on muokattavissa rakenteisempaan muotoon, esim. kyselylomakkeeksi, jossa valikoitavissa toteutettavat prosessit ja kirjattava niiden oheen tarkennukset ja lisähavainnot. Yksi esimerkkiesitys tästä on kuvassa 10 esitetty SOLEAn Kohdealueen pe-

rusprosessit ja toiminnot –tarkastuslistan pohjalta esitäytetty JHS 179 *Prosessit* –matriisi. Kaikkia eritasoisia toimintoja ja tehtäviä ei ole järkevää kuvata samaan prosessilistaukseen, vaan lähinnä prosessi- ja aliprosessityyppiset tehtävät tai työnkulut, joista on tarkoitus tuottaa tarkempia kuvauksia.

| | 2 | 3 | 4 |
|---|---|---|---|
| 1 | Prosessit | | |
| 2 | | | |
| 3 | | | |
| 4 | Prosessi | Tärkeys | Kuvaus |
| 5 | 1.1. Työntekijän työsuhteen aloittaminen | | |
| 6 | 1.2 Työntekikän aseman muuttaminen | | |
| 7 | 1.3 Työntekijän työsuhteen päättäminen | | |
| 8 | 1.4 Käyttövaltuuksien hakeminen | | |
| 9 | 1.5 Käyttövaltuuksien puoltaminen ja hyväksyminen | | |
| 10 | 1.6 Käyttövaltuuksien poisto | | |
| 11 | 1.7 Edustajuuden ylläpito | | |
| 12 | 1.8 Unohtuneen salasanan palauttaminen tai uusiminen | | |
| 13 | | | |
| 14 | | | |

**Kuva 10**: JHS179 *Prosessit* –matriisi (indeksointi ja arvot *SOLEA Kohdealueen perusprosessit ja toiminnot* –tarkastuslistasta).

***Yhteenveto välineellä saavutetuista tuloksista:***
- valinta ja tarkennuksia projektissa toteutettavien prosessein ja työnkulkujen suhteen

***Tulosten kirjaaminen***
- mallin ohessa JHS 179-ProsessiT -matriisi

## 2.4 Tarkastuslista keskeisimmistä suunnittelupäätöksistä sovellusalueelle

**Menetelmä tai väline**

dokumentin luku: *6 Käyttäjähallinnan keskeisiä suunnittelupäätöksiä*

# 6 Käyttäjähallinnan keskeisiä suunnittelupäätöksiä

Käyttäjä- ja pääsynhallinnan arkkitehtuurin määrittelemiseksi on tehtävä joukko keskeisiä suunnittelupäätöksiä. Tässä luvussa esitetään etenkin sovellus- ja arkkitehtuurinäkökulmasta tähän liittyviä keskeisiä suunnittelupäätöksiä. Keskeisimmät päätökset ovat:

- mitkä toiminnot, työnkulut tai prosessit pyritään yhdenmukaistamaan tai automatisoimaan?
- mitkä palvelut ja järjestelmät otetaan keskitetyn käyttäjä- ja valtuushallinnan tai kertakirjautumisen piiriin?
- missä määrin eri käyttäjäryhmiä ja myös käyttäjien ja sovellusten pääsynhallintaa pyritään kehittämään samoilla ratkaisuilla?
- millaisia turvatasoja määritellään (huomioiden mm. tunnistamisen vahvuus, roolien ja käyttäjäattribuuttien tarkkuus ja monimuotoisuus sekä pääsynhallinnan vahvuus, ks. alla) eri käyttäjäryhmille?

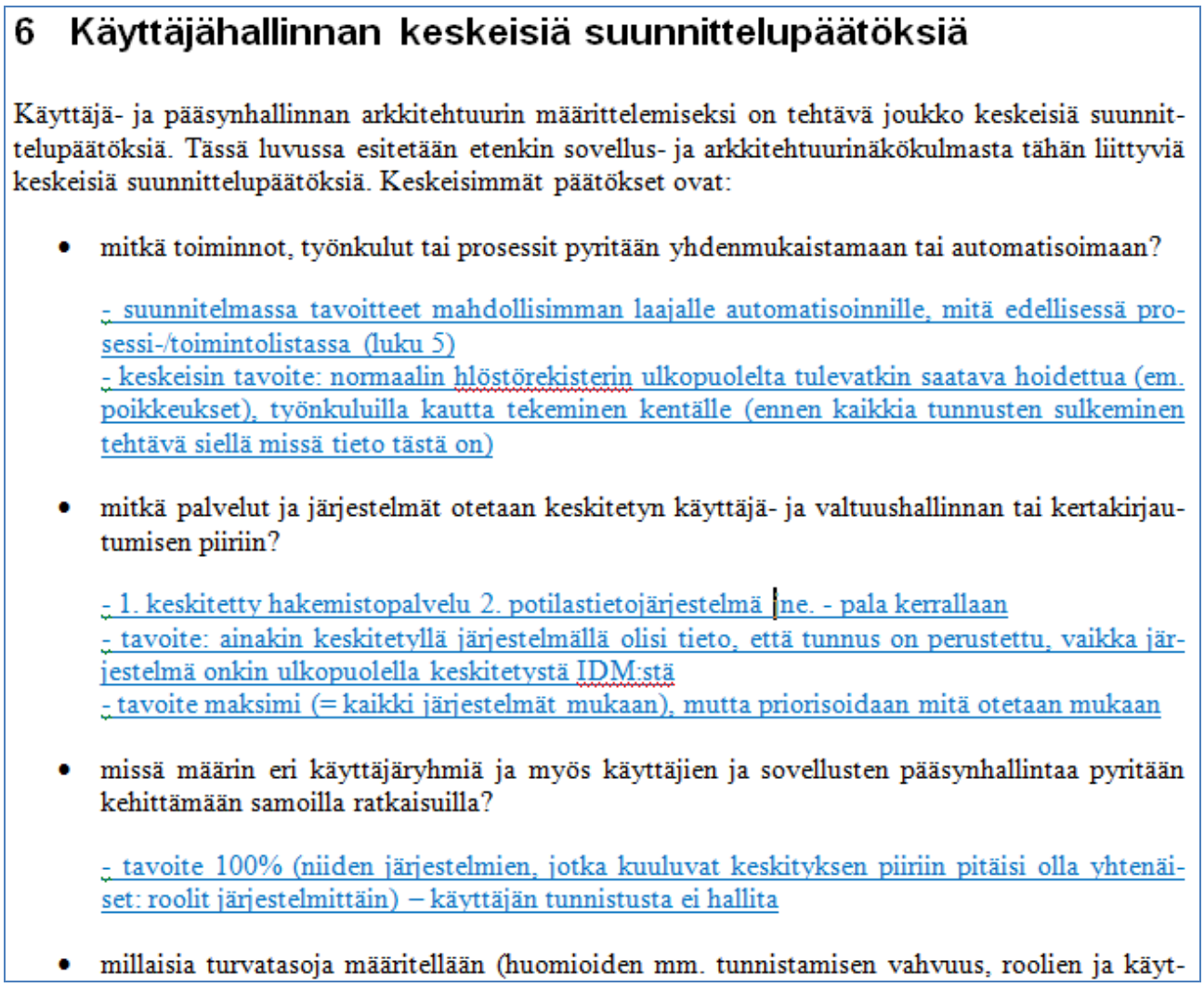
**Todentamisen vahvuustasot**

**Kuva 11**: Esimerkkiotos *Tarkastuslista keskeisimmistä suunnittelupäätöksistä* sovellusalueelle.

**Menetelmän tai välineen hyödyntäminen**

Alustukseksi menetelmän selvittäminen osallistujille jonka jälkeen keskustelu: listatuista suunnittelupäätöksistä ja miten ne ratkaistaan tulevassa järjestelmässä? Keskustelun tulokset ja päätöksiin näihin liittyvät havainnot ja tarkennukset kirjattiin dokumenttipohjaan.

**Menetelmällä tai välineellä saavutetut tulokset**



6 Käyttäjähallinnan keskeisiä suunnittelupäätöksiä

Käyttäjä- ja pääsynhallinnan arkkitehtuurin määrittelemiseksi on tehtävä joukko keskeisiä suunnittelupäätöksiä. Tässä luvussa esitetään etenkin sovellus- ja arkkitehtuurinäkökulmasta tähän liittyviä keskeisiä suunnittelupäätöksiä. Keskeisimmät päätökset ovat:

- mitkä toiminnot, työnkulut tai prosessit pyritään yhdenmukaistamaan tai automatisoimaan?

  - suunnitelmassa tavoitteet mahdollisimman laajalle automatisoinnille, mitä edellisessä prosessi-/toimintolistassa (luku 5)
  - keskeisin tavoite: normaalin hlöstörekisterin ulkopuolelta tulevatkin saatava hoidettua (em. poikkeukset), työnkuluilla kautta tekeminen kentälle (ennen kaikkia tunnusten sulkeminen tehtävä siellä missä tieto tästä on)

- mitkä palvelut ja järjestelmät otetaan keskitetyn käyttäjä- ja valtuushallinnan tai kertakirjautumisen piiriin?

  - 1. keskitetty hakemistopalvelu 2. potilastietojärjestelmä ne. - pala kerrallaan
  - tavoite: ainakin keskitetyllä järjestelmällä olisi tieto, että tunnus on perustettu, vaikka järjestelmä onkin ulkopuolella keskitetystä IDM:stä
  - tavoite maksimi (= kaikki järjestelmät mukaan), mutta priorisoidaan mitä otetaan mukaan

- missä määrin eri käyttäjäryhmiä ja myös käyttäjien ja sovellusten pääsynhallintaa pyritään kehittämään samoilla ratkaisuilla?

  - tavoite 100% (niiden järjestelmien, jotka kuuluvat keskityksen piiriin pitäisi olla yhtenäiset: roolit järjestelmittäin) – käyttäjän tunnistusta ei hallita

- millaisia turvatasoja määritellään (huomioiden mm. tunnistamisen vahvuus, roolien ja käyt-

**Kuva 12**: Esimerkki välineen käytöstä, haastattelijan tekemät merkinnät nähtävissä sinisellä alleviivattuina.

**Arviointi ja näkemykset**

Vastauksien sijoittaminen JHS 179-kuvauskehikkooon vastaavasti kuin muidenkin menetelmien ja välineiden kohdalla tässä dokumenttiosiossa vaatii hieman enemmän tulkintaa ja on myös riippuvainen siitä missä vaiheessa projektia ja millä tasolla keskustelu käydään.

Kuten jo aiemmin mainittu kartoitusvaiheessa projektia linjauksien ja vaihtoehtoja pois sulkevien päätöksien tekeminen useissa tapauksissa ei vielä kannata, kartoitusvaiheessa päätöksiä varten vasta kerätään tietoa, jonka pohjalta informoidut päätökset tehtävissä. Tästä johtuen osion tarkemmat suunnittelupäätökset, kuten jo teknologia- ja standardilinjauksiin menevät osiot, esim. *SOA-ympäristöissä korostuvia suunnittelupäätöksiä* –osio, päädyttiin jättämään käsittelemättä.

Toisena vaikuttavana tekijänä läpikäynnin tuloksiin nähtiin myös läpikäynnin formaaliuden taso: esim. kartoitusvaiheessa ei nähty järkeväksi asettaa rajauksia sille mihin suuntaan keskustelu etenee, vaan kaikki ratkaisumalleja yms. käydään läpi ja kirjataan havainnot sitä mukaa kun niitä ilmenee.

Edellä kuvatut havainnot peilautuvat vahvimmin tällä välineellä saaduissa vastauksissa, joita nähtävissä kuvassa 12 näkyvistä muistiinpanoista. Esimerkkikatkelmasta poimittavissa, niin arkkitehtuuriperiaatteiksi yleistettäviä linjauksia, (kuva 4 JHS179 -Arkkitehtuuriperiaatteet), kuin kehittämisvaatimuksia ja -tavoitteita (vrt. kuva 5 JHS 179 -*Kehittämisvaatimukset ja tavoitteet*) sekä yksittäisiin tarkemman tason työnkulkuihin liittyviä ja järjestelmäkohtaisia tarkennuksia. Suurin osa saaduista vastauksista on nähtävissä kategorisoitaviksi ja muunnettavissa esim. Kehittämisvaatimuksiksi ja tavoitteiksi tai Arkkitehtuuriperiaatteiksi, ja sitä kautta käsiteltäviksi JHS-suosituksen mallien avulla, riippuen minkä tasoiseksi kokonaisarkkitehtuurikuvauskokonaisuudeksi JHS-malleja hyödynnettäessä tavoiteltu tuotos olisi kaavailtu, esim. joko koko organisaation kokonaisarkkitehtuuridokumentaatio tai esim. käyttäjähallinnan segmenttiarkkitehtuuri.

## 2.5 Tunnistettujen palveluiden luettelo (SOA)

**Menetelmä tai väline**

dokumentin luku: *7 Käyttäjähallinnan SOA-palvelujen tunnistaminen ja rajaus*

**Käyttäjien, roolien ja valtuuksien määrittely**

| | |
|---|---|
| Käyttäjähallintapalvelu | toiminnallinen palvelu, joka tarjoaa käyttäjien käyttäjätilitietojen ylläpitotoiminnot (mm. käyttäjien lisääminen, poistaminen, käyttäjien käyttäjätili- ja attribuuttitietojen ylläpito) |
| Käyttövaltuushallintapalvelu | toiminnallinen palvelu, jolla käyttäjät ja käyttäjätilit yhdistetään rooleihin ja käyttöoikeuksiin |
| Roolienhallintapalvelu | toiminnallinen palvelu, jolla ylläpidetään roolitietoja, sisältää myös roolirekisterin |
| Resurssienhallintapalvelu | palvelu, jonka avulla määritellään suojattavat resurssit, sovellukset ja palvelut sekä niiden käyttöön tarvittavat valtuudet; voi liittyä käyttövaltuushallintapalveluun |
| Käyttäjähakemisto | hakemisto, joka tarjoaa pääsyn ainakin keskeisiin käyttäjähallintapalvelun kautta ylläpidettyihin tietoihin; hakemiston rajapintojen avulla voidaan kysellä käyttäjätietoja |
| Metahakemisto | hakemisto, joka yhdistää useiden muiden käyttäjä- tai henkilöhakemistojen tietoja ja sisältää niiden välisten suhteiden määrittelyt |
| Käyttövaltuusrekisteri | tietopalvelu, joka säilyttää ja palauttaa tiedon käyttäjien käyttövaltuuksista |

**Kuva 13**: esimerkki aihealueittain ryhmitellyistä palveluista

**Menetelmän tai välineen hyödyntäminen**

Alustukseksi menetelmän selvittäminen osallistujille jonka jälkeen keskustelu: tulevan ratkaisun mahdollisista palveluista läpikäymällä pohjamateriaalina tunnistettujen palveluiden luettelo.

**Menetelmällä tai välineellä saavutetut tulokset**

Kartoitusvaiheessa olevassa projektissa, jossa erilaiset alusta- ja infrastruktuuriratkaisut ovat vielä avoimina (lähinnä ainoa linjaus: tarkoitus hankkia mahdollisimman valmis pakettiratkaisu), on vaikeaa tai jopa nähty turhaksi ottaa vielä kantaa tarkemman tason teknisiin yms. ratkaisuihin, kuten palvelupohjaisuuden ja sitä myöden eri palveluiden hyödyntämiseen. Todettiin, että ratkaisulle suotava piirre olisi avoimuus esim. siten, että hankittava ratkaisu tarjoaa toiminnallisuuttaan SOA-palveluina muiden sovellusten hyödynnettäväksi. Mutta ilman näiden palveluiden hyödyntämiselle asetettuja tarkempien tarpeiden selvittämistä painoarvojen asettaminen nähtiin vielä liian vaikeaksi.

**Käyttäjien, roolien ja valtuuksien määrittely**

| | |
|---|---|
| Käyttäjähallintapalvelu<br>X | toiminnallinen palvelu, joka tarjoaa käyttäjien käyttäjätilitietojen ylläpitotoiminnot (mm. käyttäjien lisääminen, poistaminen, käyttäjien käyttäjätili- ja attribuuttitietojen ylläpito) |
| Käyttövaltuushallintapalvelu<br>X | toiminnallinen palvelu, jolla käyttäjät ja käyttäjätilit yhdistetään rooleihin ja käyttöoikeuksiin |
| Roolienhallintapalvelu<br>X | toiminnallinen palvelu, jolla ylläpidetään roolitietoja, sisältää myös roolirekisterin |
| Resurssienhallintapalvelu | palvelu, jonka avulla määritellään suojattavat resurssit, sovellukset |

**Kuva 14**: Esimerkki palvelutaulukosta, mukana haastattelijan tekemät merkinnät: tehdyt valinnat kartoitusvaiheessa nähtiin merkitsevän lähinnä vastaavaa toiminnallisuuden ilmenemistä tulevassa ratkaisussa, ottamatta kantaa toteutetaanko ne SOA-tyyliin.

## Arviointi ja näkemykset

Karkeasti hahmotettujen SOA-palveluiden tarjoamat toiminnallisuudet oli tässä tapauksessa hyödynnettävissä myös ratkaisun toiminnallisten tarpeiden kartoittamisessa ts. palvelut nähty toimintoina, joita ratkaisu tulee tarjoamaan (vrt. myös edelliset mallit ja niissä suoritetut ratkaisun toiminnallisuuden kartoitukset ja jäsentämiset).

Palvelulistaus nähtiin tässäkin tapauksessa mahdolliseksi rakenteistaa, hyödyntäen valmiiksi saatavilla olevia malleja, kuvassa 15 esimerkkitoteutuksena SOLEA -käyttäjähallintapalvelulistauksen pohjalta esitäytetty JHS 179 Tietojärjestelmäpalvelut –matriisi. Toteutus vastaavalla tavalla hyödynnettävissä tarkastuslistana kartoitusvaiheessa ja jatkotyön pohjana kuin edellä esitetty *SOLEA Kohdealueen perusprosessit ja toiminnot* –tarkastuslistan mäppäys JHS179 *Prosessit* –matriisiin (Liite 1, luku 2.3).

Tietojärjestelmäpalvelut

Päiväys

Versio

| Nimi | Kuvaus | Palvelun keskeinen toiminnallisuus | Korvaa nämä palvelut / uusi | Palvelun toteuttava tietojärjestelmä | Omistajayksikkö / osasto | Vastuuhenkilö | Toiminnallinen luokitus | Strateginen merkitys | Kriittisyys | Elinkaaren tila | Palvelutaso | Muuta |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Käyttäjähallintapalvelu | toiminnallinen palvelu, joka tarjoaa käyttäjien käyttäjätilitietojen ylläpitotoiminnot (mm. käyttäjien lisääminen, poistaminen, käyttäjien käyttäjätili- ja attribuuttitietojen ylläpito) | | | | | | | | | | | |
| Käyttövaltuushallintapalvelu | toiminnallinen palvelu, jolla käyttäjät ja käyttäjätilit yhdistetään rooleihin ja käyttöoikeuksiin | | | | | | | | | | | |
| Roolienhallintapalvelu | toiminnallinen palvelu, jolla ylläpidetään roolitietoja, sisältää myös roolirekisterin | | | | | | | | | | | |
| Resurssienhallintapalvelu | palvelu, jonka avulla määritellään suojattavat resurssit, sovellukset ja palvelut sekä niiden käyttöön tarvittavat valtuudet; voi liittyä käyttövaltuushallintapalveluun | | | | | | | | | | | |
| Käyttäjähakemisto | hakemisto, joka tarjoaa pääsyn ainakin keskeisiin käyttäjähallintapalvelun kautta ylläpidettyihin tietoihin; hakemiston rajapintojen avulla voidaan kysellä käyttäjätietoja | | | | | | | | | | | |
| Metahakemisto | hakemisto, joka yhdistää useiden muiden käyttäjä- tai henkilöhakemistojen tietoja ja sisältää niiden välisten suhteiden määrittelyt | | | | | | | | | | | |
| Käyttövaltuusrekisteri | tietopalvelu, joka säilyttää ja palauttaa tiedon käyttäjien käyttövaltuuksista | | | | | | | | | | | |
| Provisiointipalvelut | palvelu, jonka avulla keskitetysti ylläpidetyt (master) käyttäjä- ja käyttövaltuustiedot voidaan levittää useisiin eri järjestelmiin; voi myös sisältää toiseen suuntaan tapahtuvaa käyttäjähallintatietojen välitystä | | | | | | | | | | | |
| Federointipalvelu | toiminnallinen palvelu, jonka avulla käyttäjien erilliset identiteetit yhdistetään luottamusverkostossa | | | | | | | | | | | |
| Käyttäjäprofiilipalvelu | palvelu, jonka kautta käyttäjän attribuutteja (mahdollisesti myös muuhun kuin pääsynhallintaan liittyen, esim. käyttäjäpreferenssit) voidaan ylläpitää ja saada niitä tarvitseville; voi olla joissakin tapauksissa yhdistettynä etenkin käyttäjähakemistoon tai käyttäjähallintapalveluun | | | | | | | | | | | |
| Valtuutusten ja suostumusten hallintapalvelut | palvelut, joilla ylläpidetään tietoa käyttäjän tai asiakkaan antamista valtuutuksista tai suostumuksista | | | | | | | | | | | |

**Kuva 15**: Esimerkki JHS 179 Tietojärjestelmäpalvelut –taulukko. Esitäytetty SOLEA-hankkeessa tunnistetuilla kohdealueen tyypillisillä tai mahdolliseksi nähdyillä SOA-palveluilla.

***Yhteenveto välineellä saavutetuista tuloksista:***
- valinta ja tarkennuksia projektissa toteutettavien palveluiden suhteen

***Tulosten kirjaaminen***
- mallin ohessa JHS 179 Tietojärjestelmäpalvelut –taulukko (listaus)

## 2.6 Palvelukuvaustaulukot sovellettuna kohdealueelle (SOA-näkökulma)

dokumentin luku: *8 Palvelukuvaustaulukot*

**8.1 Tunnistuspalvelu**

| | |
|---|---|
| Palvelun nimi | Tunnistuspalvelu (sisäinen tunnistuspalvelu) |
| Tarkoituksen lyhyt kuvaus: mitä toimintoja ja tietoja kattaa | Toiminnallinen palvelu, jonka avulla oman organisaation käyttäjä voi tunnistautua (tunnistaminen ja todentaminen)<br>**Toiminnot:**<br>palauttaa käyttäjän identiteetin sekä mahdollisesti tunnistusselosteen ja muita sovittuja käyttäjän attribuutteja tunnistetietojen perusteella.<br>Voi toimia yhdessä mm. kertakirjautumispalvelun ja sessiopalvelun kanssa. |
| Keskitys / hajautus | Nykytila: tunnistautuminen usein sovelluskohtaista.<br>Tavoitetila: keskitettyjen tunnistuspalvelujen käytön lisääminen, optimina yksi tunnistuspalvelu / organisaatio. |
| Mihin prosessiin liittyy | 2.1 tunnistautuminen, sisältäen tunnistetietojen esittämisen, tunnistamisen ja todentamisen<br>2.2 käyttäjän todentaminen, ilman tunnistetietojen erillistä esittämistä |

**Kuva 16**: Esimerkki Palvelukuvaus-taulukosta.

**Menetelmän tai välineen hyödyntäminen**

Ei käytetty vielä projektin ollessa kartoitusvaiheessa, perusteluita tarkemmin Liite 1, luku 2.5 *Tunnistettujen palveluiden luettelo (SOA)*. Välineen mahdolliseksi hyödyntämismalliksi nähtiin edellisellä mallilla (palvelulistaus) tarkennettaviksi valikoituneiden palveluiden jatkotarkentaminen ominaisuus kerrallaan (taulukon rivit).

**Menetelmällä tai välineellä saavutetut tulokset**

Ei hyödynnetty tässä läpikäynnissä (perustelut aiemmin).

**Arviointi ja näkemykset**

Ilman soveltamiskokemusta, saatuja arvioita tähän yhteyteen ei ole kirjattavissa. Sen sijaan Palvelunkuvaustaulukoiden hyödyntämiselle nähtävissä vastaavanlainen malli ja yhteys JHS 179 –suositusten mallipohjiin, kuin usealla edellä dokumentoidulla menetelmällä ja välineellä.

Palvelukohtaisien taulukoiden tiedoilla osittain edelleen täytettävissä *Tunnistettujen palveluiden luettelo –luvussa* (Liite 1, luku 2.5, kuva 15) jatkokehitysideoissa esitetty JHS179-*Tietojärjestelmäpalvelut* -taulukon tarkempien tietojen täydentäminen palveluittain (taulukon sarakkeet 2-14, suoria vastaavuuksia mm.: *Palvelun keskeinen toiminnallisuus, Toiminnallinen luokitus* jne.).

***Yhteenveto välineellä saavutettavista tuloksista:***
- tarkennuksia projektissa toteutettavien palveluiden suhteen

***Tulosten kirjaaminen***
- mallin ohessa JHS 179 Tietojärjestelmäpalvelut –taulukko (tarkennukset palveluittain)

# 3 Arkkitehtuurin kuvaustapojen case-tiedonkeruu

Seuraavissa kahdessa aliluvussa esitetään kartoitusprojektille tehdyn läpikäynnin yhteydessä hyödynnetyt *Arkkitehtuurin kuvaustapojen case-tiedonkeruulomakkeet* (Lomake *1 Perustiedot* ja Lomake *3 Kuvausten läpikäynti tasoittain*) muistiinpanoineen (haastattelijan tekemät muistiinpanot merkattu sinisellä lomakkeisiin ja monivalintojen yhteydessä valinta lisäksi alleviivattu). Käydyt keskustelut ja niiden aikana saadut johtopäätökset ovat kirjattu ja mukana dokumentaatiossa likipitäen sellaisenaan muutamaa tuotenimen ja toimijan anonymisointia lukuun ottamatta. Lomakkeet ja niihin tehdyt muistiinpanot: mm. haastattelun aikana syntyneet lukuisat muistilistat, priorisoinnit, jäsentelyt ja linjaukset jne. nähty hyödylliseksi haasteltavan toimesta ja toimitettu sellaisenaan toteutusprojektin vetäjälle hyödynnettäviksi kyseisen projektin jatkodokumentaatiossa.

## 3.1 Perustiedot-lomake

# Arkkitehtuurin kuvaustapojen tiedonkeruu, pohjataulukot
# 1 - Perustiedot

**Perustiedot**

| Kysymys | Vastaus |
|---|---|
| **Projektin / kohteen nimi** | Toimikortti/Kertakirjautuminen ja IdM (Pohjois-Savon sairaanhoitopiiri /Istekki) |
| Tietojen kokoaja | Hannu Virkanen, Juha Mykkänen, Itä-Suomen yliopisto |
| Tietolähteet | toimittajan asiantuntija/vetäjä, Istekki/tilaajan asiantuntija/vetäjjä, Pohjois-Savon sairaanhoitopiiri (27.4.) |
| Tiedonkeruun ajankohta | 27.4.2011 (jatko/muut aihepiirit-lomakkeet: 17.5., 30.5.) |

| Kysymys | Vastaus |
|---|---|
| Lyhyt kuvaus projektista johon kuvaustapojen käyttö liittyy, projektin tavoite | **Projektikokonaisuus**: kolmi(projektisuunnitelmassa:neljä) -osainen<br>- Toimikortti- ja kertakirjautuminen (projektisuunnitelmassa erilliset projektit: pilotointi ja käyttöönotto)<br>- Toimikorttien logistiikka ja toimintamallit<br>- IDM – käyttäjähallinnan selvitystyö<br>*=> SOLEAn läpikäynnissä kaikkien osaprojektien muodostama kokonaisuus ja sen käsittely yhdessä*<br><br>**tavoitteet projektikokonaisuudelle:**<br>- Toimikortti- ja kertakirjautuminen: hakemistopalvelutuotteen toimialueeseen sekä keskeisiin potilastietojärjestelmiin (käyntiin syksy 2011 - KYSterissä)<br>- Toimikorttien logistiikka ja toimintamallit: logistiikka toimimaan, syksyllä paikallisen kunnallisen toimijan eArkistopilotti (alueellinen potilastietojärjestelmä), jakelu 400 kpl korttia (vuodenvaihde 2011/2012 mennessä), ensi keväänä shp-tasolla eReseptin käyttöönotto ja sen vaatima toimikorttilogistiikka, mukana myös kertakirjautuminen toimikortilla<br>- IDM – käyttäjähallinnan selvitystyö: selvittää prosessit ja roolit, nykyprosessien kehittäminen sekä tuotteen hankinta ja käyttöönotto, tavoiteaikataulu: vuoden loppuun mennessä |

| | |
|---|---|
| | **Yhteenveto:**<br>- tavoitetilan asettelu ja siihen liittyvät poliittiset päätökset (ohjausryhmän kautta)<br><br>**Syy/motivaatio**: lakimuutokset (mm. Kanta-liittymät), joihin vastaamisen ohessa selvitettävä myös mahdollisesti saatavat hyödyt |
| Onko projektissa SOA:n käyttöön liittyviä tavoitteita tai menetelmiä | [**ei, epäselvää**]<br>- mahdollisesti seuraavissa vaiheissa (nyt vasta tarpeiden selvitys/määritysprojektit)<br>- nähtiin, että SOA mm. toimikortti/kertakirjautumisen ohessa, saattaa tulla vastaan (esim. tuotepohjaisesti – tuotteiden kautta) |
| Projektin vaihe | pääasiassa suunnitteluvaihe (pilotointi alkamassa Toimikortti-puolella) |
| Projektin osallistujat ja johto | **toimittaja**: Istekki<br>- IDM/kertakirjaus -projekti: toimittajan asiantuntija/vetäjä(johto) sekä kaksi muuta asiantuntija/toteuttajaa (mm. eReseptille omansa)<br>**asiakas/tilaaja**: PSshp<br>- yhteyshenkilö: tilaajan asiantuntija/vetäjä, lisäksi asiantuntija (ex-KYS/nyk-Istekki) sekä mahdollisesti jatkossa paikallinen kunnallinen toimija tulossa mukaan<br>- ohjausryhmä: vielä nimeämättä, vaatii suunnitelmien kypsymisen (arvio n.: 8/2011) |
| Missä määrin kohde on jokin seuraavista | a) arkkitehtuurikokonaisuuden hallinta<br>**b) rajatun prosessin tai kehittämiskohteen arkkitehtuurikuvaukset tai määrittelyt**<br>c) integraatioprojektin arkkitehtuurikuvaukset tai määrittelyt |
| Onko käytössä / pohjana jokin yleinen arkkitehtuurikehikko | Ei, tehdään mukaillen asiakkaan (shp/paikallisen kunnallisen toimijan) menetelmiä<br>- (toimittajalla ei vielä omaa – tarvittaisiin/toiveissa jatkossa) |

**Arkkitehtuurityön taustatiedot**

| **Kysymys** | **Vastaus** |
|---|---|
| Arvio, kuinka paljon arkkitehtuurikuvauksia organisaatiossa on tuotettu aiemmin | - projektikohtaista dokumentaatiota runsaasti, mutta ei käyttäjähallintaan arkkitehtuurikuvauksia |
| Onko organisaatiolla määritelty ”ylemmän” tason arkkitehtuureita | - löytyy osia esim. sovellusarkkitehtuurista järjestelmäkartta (ajantasaisuus – ei tiedossa vrt. tietojärjestelmärekisteri alla) |
| Onko kuvausmenetelmiä standardoitu organisaatiossa | - ei, yleensä projektikohtaiset valinnat<br>- lähinnä standardoitua mallia: tietojärjestelmärekisteri (ei ole prosessia ylläpitoon) |
| Lyhyt kuvaus, millaista ohjausta tai johtamista arkkitehtuurityöhön on käytetty | - hallittu projektikohtaisesti (ei projektin elinkaaren ylittävää ylläpitoa)<br>- puuttuu myös projektinhallintajärjestely (esim. dokumenttiarkisto) |
| Tärkeimmät valmiina hyödynnettävät kuvaukset tai ohjeet ja mistä ne saadaan? | projektin pohjadokumentaationa mm.:<br>- SOLEA-yms. pohjadokumenttien avulla aloitettu aihealueen selvitystyö asiakasorganisaatiossa (työpaperi vuodelta 2008)<br>- muiden shp:n vastaava työ<br>- eri toimittajien materiaali<br>- kuvauksia toimikortin osalta (soveltaen paikallisen kunta-toimijan käytäntöjä) |

**Tavoitteet**

| Kysymys | Vastaus |
|---|---|
| Kuvausten käyttötarkoitus lyhyesti | - uusien palvelujen tai ohjelmistojen määrittely (tärkein)<br>- toiminnan muuttaminen (tavoitetilan kuvaaminen, esim. toimikorttien käyttöön otto: muuttaako rutiineja? - toiseksi tärkein)<br>- kehityskohteiden löytäminen<br>- toiminnan tehostaminen (esim. käyttäjätunnukset nopeammin)<br>- organisaation kehittäminen<br>- käyttöönoton suunnittelu<br>- lainsäädännön vaateiden täyttäminen (ja ohessa tavoitteena myös parantaa toimintaa muutoksilla)<br>- viestintä eri sidosryhmien välillä (erillinen osio/osa vaatimuksiksi hankintoihin) |
| Kuvausten hyödyntäjät | 1) tietohallinnon asiantuntijat/muut työntekijät (mm. suunnittelu- ja hankintadokumenteiksi, käyttöönottojen ja toimintamallien hahmottelu ja syötteet myöhemmälle tarkentamiselle, mm. käyttöpolitiikat, priorisoinnit – esim. mitkä järjestelmät otetaan IDM-järjestelmän/kertakirjautumisen piiriin, mitä ulosjääville tehdään, tarvittaessa ratkaisuvaihtoehtojen kuvauksia)<br>2) ulkoiset konsultit tai asiantuntijat<br>3) organisaation johto<br><br>projektin tuotoksille nähdään seuraavia eritasoisia jatkohyödyntämismahdollisuuksia (ts. saatavat kuvaukset toimivat syötteenä mm.):<br>- johtotasolle tuleva erillinen/kohdennettu/tiivistetty viestintä (ppt yms.–tyyppistä) => johdon tuen saaminen/sitouttaminen hankkeeseen<br>- ohjeistukset työntekijöille (esim. toimikortti-puoli)<br><br>käyttävätkö kuvausten tekijät itse tuotoksia:<br>- kyllä, pohjadokumentteina tuleviin projekteihin |
| Kuvausten uudelleenkäyttö | - kyllä, ks. edellinen kohta: suunnitelmia tarkennetaan tulevissa projekteissa mm. hankintoja varten<br>- mahdollisesti muita tulevia tarpeita: mm. uusien osapuolten mukaan tulo (paikalliset kuntatoimijat) ja terveydenhuolto-organisaatioiden mahdolliset uudelleen järjestäytymiset (esim. Erva-alueella) |
| Kuvausten tuottajat | tietohallinnon asiantuntijat |
| Kuvausten tekemiseen käytetyt tietolähteet | nykykäytäntöjen ja tarpeiden kartoituksessa hyödynnetty:<br>- IDM-osuus: tietohallinnon edustajat (KYS)<br>- osastonhoitaja-sihteeri<br>- henkilöstöhallinto (työvoimapalvelut, hallintosihteeri, henkilöstöhallinnon-järjestelmä)<br>- Istekkin IDM-asiatuntijat<br>- harjoittelijoiden suhteen: Savonia-AMK:n ja Itä-Suomen yliopiston opetushoitaja(/sihteeri) |
| Kuvausten tekemiseen käytetyt välineet | käsin tehdyt muistiinpanot => Word-dokumenteiksi |
| Missä määrin projektin tavoitteet tulevat seuraavilta tahoilta (arvio)[3] | - 70% tietohallinto (KYS ja Istekki: ICT-palvelujen kokonaistuottaja)<br>- 30% muut: käyttäjät / työntekijät / johto |

[3] tarvittaessa lomakkeen 3 täyttämisen jälkeen voidaan tehdä tarkempi lähtökohta-analyysi, esim. 1. tietohallintolähtöinen (esim. järjestelmän uusiminen, miten liitytään kansallisten palvelujen käyttöön, arkkitehtuurin hallintamallien kehittäminen); 2. liiketoimintalähtöinen (esim. organisaatiomuutos, toiminnan tuoton tai kannattavuuden parantaminen, organisaation johdon asettamat päätavoitteet ja vaatimukset), 3. käyttäjälähtöinen (esim. tiedonsiirron kehittäminen tietyssä prosessissa, organisaation sisäisten käyttäjien tai

| | |
|---|---|
| Missä määrin kuvaaminen kohdistuu tavoitetilaan, missä määrin nykytilaan, missä määrin siirtymäpol-kuun (arvio) | - 20 % nykytila (tarpeen mukaan)<br>- 50 % migraatio tai siirtymäpolku<br>- 30 % tavoitetila<br><br>tavoitetilan ajankohta:<br>- ei aikataulutettua loppua projektille<br>- vaihtelee kohteittain esim.: kansallisten palveluiden aikataulutus vaikuttaa, mutta ei ole sama aikataulu, IDM/AD:n toteutus ensi vuoden alussa jne.<br>- ~vuoden päästä pitää olla esittää konkretiaa |
| Rajaukset | rajaus yksiköiden suhteen:<br>- kaikki shp:n yksiköt ja sairaalat: kerta- ja toimikorttikirjautumiseen mukaan<br>(- vaiheistus: ensin lääkärit korttikirjautumiseen, sitten terveydenhuoltohenki-löstö, sitten muu henkilökunta)<br><br>rajaus käyttöoikeuden/henkilöstön mukaan<br>- mukaan kaikki jolla käyttöoikeus<br>- myös esim. opiskelijat ja ulkoiset toimijat (toimittajien edustajat, tutkijat joilla ei työsuhdetta sekä n. 1000 muiden terveyskeskusten käyttäjiä)<br>- ostopalvelujen tuottajat<br>- henkilöstöjärjestelmässä vain henkilöt, jotka saavat korvauksen palkan muodossa, sen ulkopuolisia käyttäjiä n. 1000 + 1000 opiskelijaa<br>-organisaation ulkoiset käyttäjät ovat mukana tavoitetilan asettelussa<br><br>rajaus järjestelmien suhteen:<br>- ei vielä rajauksia ovatko kaikki järjestelmät mukana<br><br>- rajaus vaatimusten tarkkuustasoon: hankinnan edellyttämä tarkkuustaso = toiminnalliset ominaisuudet riittävät hankinnan kriteereiksi |

asiantuntijoiden asettamat päätavoitteet ja vaatimukset). Myös tavoitetila / nykytila / siirtymä-analyysi voidaan tarkentaa lopullisesti haluttaessa tiedonkeruun ja kuvausten analyysin jälkeen.

### 3.2 Kuvausten läpikäynti tasoittain -lomake

# Arkkitehtuurin kuvaustapojen tiedonkeruu, pohjataulukot
# 3 - Kuvausten läpikäynti tasoittain
**Perustiedot**

| Kysymys | Vastaus |
|---|---|
| **Projektin / kohteen nimi** | Toimikortti/Kertakirjautuminen ja IdM (Pohjois-Savon sairaanhoitopiiri /Istekki) |
| Tietojen kokoaja | Hannu Virkanen, Juha Mykkänen (mukana 17.5.2011), Itä-Suomen yliopisto |
| Tietolähteet | toimittajan asiantuntija/vetäjä, Istekki |
| Tiedonkeruun ajankohta | 17.5.2011 ja 30.5.2011 |

Yksi kuvaus voi ottaa kantaa useaan kuvattavaan seikkaan, jolloin se on listattuna useissa kohdissa. Esimerkkejä joistakin kuvaustavoista on poimittu eri kohtiin. Kaikki esiin nousevat kuvaukset lisätään lomakkeen 2 luetteloon. "Tehdään / käytetään / ei kuvata" vaihtoehdoista yhden valinta tehdään nimenomaisesti tarkasteltavana olevan projektin tai kohteen kannalta. Liitteiden 4 (Archimate) ja 5 (TOGAF) kuvausten kohteita ja kuvastapoja voidaan käyttää vastausten jäsentämisessä.

**HUOMIO**: suurin osa lomakkeella listatuista kuvauksista nähtiin hyödyllisiksi tuottaa ainakin jossain vaiheessa osana laajaa projektia(/projektikokonaisuutta), mutta projektin aikataulun/resurssien takia niiden kaikkien tuottaminen projektin kartoitusvaiheessa nähtiin haasteelliseksi (tarve priorisoinnille esim. projektin vaiheistuksen mukaan ja mm. missä vaiheessa kuvauksiin tarvittavat tiedot ovat selvillä).

**TASO: BUSINESS**

| Kuvauksen kohde | Tila |
|---|---|
| Organisaation toiminnan arvo tai lisäarvo ja niiden muodostuminen | tehdään / käytetään / ei kuvata<br>*kuvaustavat*<br>*-esim. Driver/Goal/Objective catalog, arvoketjukuvaus, value proposition, JHS: kehittämisvaatimukset ja tavoitteet*<br><br>- tehdään projektin vaikutusalueen (käyttäjä/käytönhallinta jne. - domain) näkökulmista, suhteessa organisaation toimintaan.<br>- projekti ei tarvitse suurta panosta toteuttamispäätöksen perusteluksi: suuri osa tehtävistä on lain velvoittamia (esim. eResepti=>toimikortti), mutta arvon muodostumisen kuvaus auttaa resursoimaan projekti(t) kunnolla<br>- esim. kuvaukset/joku näistä: [TOGAF: Driver/Goal/Objective catalog, arvoketjukuvaus, value proposition, JHS: kehittämisvaatimukset ja tavoitteet] hyödynnettävissä yleisesti projektidokumentaatiossa: esim. projektisuunnitelmissa ja arkkitehtuurikuvauksissa<br>- mm. tavoitteet: luettelointi ja niiden priorisointi, ajurit (esim. lait) jne.<br>- joistain osa-alueista, kuten kertakirjautuminen nähtiin voitavan laskea myös rahallisia arvioita saatavalle hyödylle |
| Organisaatiot, yksiköt, niiden roolit, suhteet, maantieteellinen sijoittuminen, kumppanit | tehdään / käytetään / ei kuvata<br>*kuvaustavat*<br>*-esim. Organization/Actor catalog, Role catalog, Location catalog, organisaatiokaavio, sijaintikaavio, JHS: sidosryhmät, JHS: organisaatiot ja sidosryhmät, JHS: toimijat-tiedot*<br><br>Roolit:<br>- organisaation varsinaisille työntekijöille annettavista rooleista tulee oma luettelo (pohjana käytetty peruspotilastietojärjestelmän työrooleja sekä henkilöstöhallintojärjestelmän titteleitä) |

| | |
|---|---|
| | - organisaation ulkopuolisille toimijoille, joille annetaan pääsy järjestelmiin oma rooliluettelo, samoin opiskelijoille omansa<br>Organisaatio:<br>- kuvataan tai hyödynnetään esim. henkilöstöhallinnosta (luettelo)<br>=> em. kahden yhdistelmämatriisi (roolit/organisaatio) = roolikartta, joka kuvaa miten organisaatiorakenne vaikuttaa käyttäjähallintaan<br><br>- sijaintiluettelo: optiona esim. kulunvalvonnan suhteen sekä huomioitava suunnittelussa organisaation hajautuneisuus, kuitenkaan ei tässä vaiheessa ykkösprioriteetti<br>- rajaus: toteutuksessa ei rajausta pääsyyn pyritä tekemään käsiteltävien tietojen suhteen, vaan rajataan pääsy järjestelmiin (joissa pääsynvalvonta tietojen suhteen) |
| Tuotteet, organisaation tuottamat palvelut, sopimukset | tehdään / käytetään / ei kuvata<br>*kuvaustavat*<br>*- esim. Product catalog, Business Service/Function catalog, Contract catalog, JHS: palvelut*<br><br>- jatkossa (tuotteistusvaiheessa/projektissa) palvelulle tullaan jatkossa tuottamaan palvelunkuvaus<br>- palvelunkuvausta tullaan hyödyntämään myös sopimuksissa liittyen palvelun toimittamiseen - vaatii hankintapäätökset jne. ts. ei myöskään tässä vaiheessa<br>- ts. projektin tämän vaiheen tuotokset vaikuttavat vasta välillisesti palvelunkuvaus-sopimus yms. lopputuotoksiin<br>(- rajaus: asiakasorganisaation palveluita ei kuvata projektissa) |
| Prosessikartta, prosessikuvaukset, organisaation toiminnot, yhteistoiminta, liiketoimintatapahtumat | tehdään / käytetään / ei kuvata<br>*kuvaustavat*<br>*-esim. Process catalog, Business Service/Function catalog, prosessikaaviot, prosessikuvaukset, JHS: prosessit, JHS: prosessit-tiedot, JHS: prosessit-järjestelmät*<br><br>- nykytila: löytyy osittain käyttäjähallinnan prosessi- ja työnkulkukuvauksia tekstimuodossa (tehty mm. haastattelujen perusteella)<br>- tavoitetila: tullaan kuvaamaan kaavioina (työnkulku- ja prosessi-tasoilla)<br>• priorisointi: ensin erikois-/poikkeustapaukset esim. määräysten päättymiset, virkavapaudet, sijaisuudet<br>• em. erikoistapausten selvityksessä nostettavissa esiin myös yleisiä linjauksia/policyjä ylemmälle tasolle, joista projektiryhmän tekemät ehdotukset hyväksytetään projektin johtoryhmällä<br>• hankeen eri osaprojekteissa (Toimikortti/Kertakirjautuminen ja IdM) tullaan tuottamaan omat prosessikuvaukset<br>• hyödynnetään SOLEA-käyttäjähallinan toiminto- ja prosessilistauksia pohjina toimintojen palastelussa sekä toteutuksen priorisoinnista<br>• tavoitteena kehittää myös uusia prosesseja käyttäjähallinnan suhteen, esim.: jatkossa yksi prosessi ja malli liittää järjestelmiä keskitettyyn käyttäjähallintaan – hyödynnettävissä jatkossa esim. tarjouspyynnössä (vaatimus) => esim. vain yksi mallin mukainen käyttäjätunnuksen perustamisprosessi |

| | |
|---|---|
| Toiminnan kannalta olennaiset tietokokonaisuudet, niiden merkitykset ja esitystavat | tehdään / käytetään / ei kuvata<br>*kuvaustavat*<br>*-esim. Data Entity/Data Component catalog, JHS: käsitemalli*<br><br>- tiedot kuvataan kohdealueen osalta: IdM-ratkaisun tietosisältöjen määrittely<br>• kuvaus: taulukko/matriisi-esitys |
| Yhteiset tai yleiset sanastot ja nimikkeet | -tehdään / käytetään / ei kuvata<br>*kuvaustavat*<br>*-esim. JHS: Sanastot*<br><br>- käsitteet: yleisenä sanastona hyödynnetään liki suoraan SOLEA-käyttäjähallinnan Keskeisiä käsitteitä (kooste JHS yms. lähteistä), tuotetaan hyödynnettäväksi kaikissa dokumenteissa |

**TASO: APPLICATION**

| **Kuvauksen kohde** | **Tila** |
|---|---|
| Sovellukset / järjestelmät | *tehdään?* / käytetään / ei kuvata<br>*kuvaustavat*<br>*-esim. Application Portfolio catalog, service catalog, sovelluskuvaukset, JHS: loogiset tietovarannot, JHS: tietojärjestelmäpalvelut, JHS: tietojärjestelmäsalkku, JHS: järjestelmät-tiedot, JHS: prosessit-järjestelmät*<br><br>- nykytila:<br>a) järjestelmäkartta: vanhentunut (sis. 250 järjestelmää, mm. tietokantariippuvuudet)<br>b) käyttäjähalllinnan näkökulmasta tehty: keskeisimmät tietojärjestelmät (ajantasaisempi Word-dokumentti, tietoja mm.: missä ylläpito kunkin järjestelmän käyttäjätunnuksille)<br><br>tavoitetila:<br>- järjestelmäkartta IDM-järjestelmän suhteen päivittyy liitettävien järjestelmien kautta (ei ykköprioriteetti) |
| Sovelluspalvelut tai -komponentit | *tehdään?* / käytetään? / ei kuvata<br>*kuvaustavat*<br>*-esim. service catalog, sovelluspalvelukuvaukset, JHS: tietojärjestelmäpalvelut*<br><br>havaintoja/poimintoja:<br>- määritys/kartoitusvaiheessa ei vielä kyetä varmuutta mitä tarpeita palvelupohjaisille toiminnoille on – tavoitteena mahdollisimman tuotepohjainen hankinta (ja sen tarjoamien palvelujen hyödyntäminen)<br>- läpikäynnissä tarkasteltiin SOLEA-käyttäjähallinta –dokumentin lukua: *7 Käyttäjähallinnan SOA-palvelujen tunnistaminen ja rajaus*, todettu sen olevan hyödynnettävissä pohjina esim. tuotteen hankintakriteeristössä – mitä ominaisuuksia (palveluita) hankittavassa tuotteessa tulisi olla<br>- esim. federointipalvelu ei tule hankintaa IDM:n kautta vaan hyödynnetään esim. HAKA-federaatiota ja Idm-järjestelmästä rakennetaan liitynnät siihen<br>- rajaus: projektissa keskitytään käyttäjähallintaan / pääsyn rajaamiseen järjestelmätasolla - pääsynvalvonta esim. tietoihin tapahtuu yhä järjestelmien kautta |

| | |
|---|---|
| Rajapintojen liittyminen toisiinsa, sovellusten tai komponenttien yhteistoiminta (collaboration) | tehdään / käytetään / ei kuvata<br>*kuvaustavat*<br>*-esim. Interface catalog, rajapintakartat, rajapintakuvaukset, integraatioarkkitehtuurikuva, JHS: liittymät ja rajapinnat*<br><br>- tässä vaiheessa ei integraatioarkkitehtuurikuvia<br>- rajapintojen suhteen IDM-tuotteen tarve pystyä tukemaan mahdollisimman joustavasti ja paljon järjestelmiä (miten pääsee kohdejärjestelmien käyttäjähallintaan), tarvitsee:<br>• laajat liityntämahdollisuudet käyttäjätietoja sisältäviin tietojärjestelmiin ja -kantoihin<br>• saatavilla olevia liityntäadaptereita/-konnektoreita keskeisimpiin liitettäviin tietojärjestelmiin (pohjana käyttäjähallinnan näkökulmasta tehty: keskeisimmät tietojärjestelmät -listaus) |
| Sovellusten ja käyttäjän vuorovaikutus, sovellusten käyttäjälle tarjoama toiminnallisuus | tehdään / käytetään / ei kuvata<br>*kuvaustavat*<br>*-esim. käyttöliittymäkuvaukset, toimintojen määrittelyt, järjestelmien käyttötapauskuvaukset*<br><br>- ei  vielä tarkkoja suunnitelmia<br>- tavoitteena Idm-tuotteen oletuskäyttöliittymien hyödyntäminen |
| Tietokokonaisuudet, joita käsitellään sovellusten avulla | tehdään / käytetään / ei kuvata<br>*kuvaustavat*<br>*-Data Entity/Data Component catalog, JHS: informaatiosalkku, JHS: toimijat-tiedot, JHS: prosessit-tiedot, JHS: järjestelmät-tiedot*<br><br>käsitelty jo ks. kohta: *BUSINESS: Toiminnan kannalta olennaiset tietokokonaisuudet, niiden merkitykset ja esitystavat* eli:<br>- IdM-ratkaisun tietosisältöjen määrittely |
| Terminologiat ja koodistot, joita hyödynnetään tietokokonaisuuksissa ja sovelluksissa | *tehdään*? / käytetään / ei kuvata<br>*kuvaustavat / viittaukset*<br><br>- tarkentuu myöhemmin lähempänä toteutusta<br>- tunnistettu jo olemassa olevia hyödynnettäviä koodistoja esim. henkilöstöhallintojärjestelmästä: koodistot kustannuspaikoista, yksiköistä, työsuhteen päättymisen syyt, tittelit jne. |

**TASO: TECHNOLOGY**

| **Kuvauksen kohde** | **Tila** |
|---|---|
| Laitteet, verkot, verkon solmut ja niiden väliset yhteydet | tehdään / käytetään / ei kuvata<br>*kuvaustavat*<br>*-esim. JHS: teknologiasalkku*<br><br>- ei tehdä kartoitusvaiheessa, tarpeen palvelun ollessa tuotannossa |
| Ohjelmistoympäristöt, järjestelmäohjelmistot | tehdään / käytetään / ei kuvata<br>*kuvaustavat*<br>*-esim. Application Portfolio catalog, JHS: teknologiakomponentit,*<br><br>- järjestelmätasolla sovelluskartat (sama: ks. *APPLICATION: Sovellukset / järjestelmät* -kohta) |

| | |
|---|---|
| Verkon solmuissa saatavilla olevat palvelut ja rajapinnat | tehdään / käytetään / ei kuvata<br>*kuvaustavat*<br>*-Application Portfolio catalog, JHS: fyysiset tietovarannot, JHS: teknologiapalvelut*<br><br>- palveluita sovelluskartassa sovellusten yhteydessä (oleellisia kuvassa vain keskeisten järjestelmien käyttäjähallintapalvelut) |
| Standardit, määrittelyt, dokumentaatio, joita hyödynnetään ohjelmistokehityksessä tai käyttöönotossa | tehdään / käytetään / ei kuvata<br>*kuvaustavat*<br>*esim. -Technology Standards catalog, JHS: standardisalkku*<br><br>- ei tarvetta listata, eikä myöskään jatkossa (esim. aihealueella olevat LDAP, HAKA tms. jo tiedossa) |

**MUUT KUVAUSTEN KOHTEET**

| **Kuvauksen kohde** | **Tila** |
|---|---|
| Kehittämisen ohjaus | *tehdään*? / käytetään / ei kuvata<br>*kuvaustavat*<br>*-esim. Architecture principles, JHS: standardisalkku, JHS: sidosarkkitehtuurit, JHS: strategiat*<br><br>- projektin aikana nähtiin rakentuvan arkkitehtuuriperiaatteita, kuten yhtenäinen rooli-malli järjestelmille sekä yhtenäinen liittämismalli järjestelmille IDM-järjestelmän piiriin |

**KUVAUSTEN ANALYYSI JA YHTEENVETO (lomakkeiden 1-3 pohjalta)**

| | |
|---|---|
| **Kuvausten painopiste** | tärkeysjärjestyksessä seuraavat (nähty, että eri sidosryhmille tämä voi olla huomattavasti erilainen)<br>1) organisaation toiminnan tai työskentelyn kehittäminen<br>2) tietojärjestelmien kehittäminen tai integrointi<br>3) tekninen infrastruktuuri<br>4) liiketoiminnan tavoitteet |
| **Arvio arkkitehtuuriohjauksen tasosta** | *esim. projektikohtainen, joitakin yhteisiä kuvauksia tai ohjeita, arkkitehtuurikäsikirja, arkkitehtuurikatselmoinnit*:<br><br>- tällä hetkellä projektikohtainen lähestyminen, mutta tunnistettu koko organisaatiolle soveltuvia malleja – vastaava etenemistapaa laajemminkin<br>– työssä nähtiin myös aineksia kokonaisarkkitehtuurityön alulle (alkutilanne: tiedostaen tehtyä arkkitehtuurityötä ei ole) |
| **Case-kohtaiset kehitysideat** | palaute läpikäytyjen kuvausten suhteen:<br>- tilanne (5/6-2011): hankkeessa menossa käyttäjähallinnan tavoitetiladokumentin laatiminen (hankintakriteeristö), jonka perusteella hankintapäätösehdotus. Materiaalia hyödynnetään tukimateriaalina myös kommunikoinnissa liiketoimintatasolle ja em. hankintapäätöksen hakemisessa, tämä kuitenkin vaatii vielä materiaalin räätälöimistä myös liiketoiminta-tasolle viestintään soveltuvaksi.<br><br>tärkeimmät kuvauskohteet jatkossa:<br>1) käyttäjähallinnan prosessikuvaus tavoitetilassa<br>2) tekniset kuvaukset uudelle hankittavalle järjestelmälle<br>3) järjestelmien liittämisen priorisointi (sovelluslistausten pohjalta)<br>4) roolityö: käyttäjähallinnan suhteen / liitettävät järjestelmäkohtaiset sovittamiset (selkeinä jo muutamien järjestelmien osalta, minkä pohjalta luodaan yleinen kartta järjestelmärooleista – sen soveltaminen tuleviin jär- |

| | |
|---|---|
| | jestelmiin esim. hyödynnetään hankinnoissa (vaatimuksena), samoin kuin toisena luotava autentikaatio/autorisointi-malliakin)<br><br>Suurin osa lomakkeella listatuista kuvauksista nähtiin hyödyllisiksi tuottaa ainakin jossain vaiheessa osana laajaa projektia(/projektikokonaisuutta), mutta projektin aikataulun/resurssien takia niiden kaikkien tuottaminen projektin kartoitusvaiheessa nähtiin haasteelliseksi (tarve priorisoinnille esim. projektin vaiheistuksen mukaan ja mm. missä vaiheessa kuvauksiin tarvittavat tiedot ovat selvillä). |
| **Tiedonkeruun kehitys-ideat** | -nähty, että lomakeläpikäynnin tueksi olisi hyvä olla domain-kohtaista tukimateriaalia (tässä casessa käyttäjähallinnan-alueella hyödynnettyä SOLEAn tuottamat arkkitehtuuri/määritys framework/sen osia: SOLEA - Vaatimukset ja rajaukset palvelupohjaiselle käyttäjä- ja käytönhallinnalle)<br>- kuitenkaan domain -kohtainen yleinen mallikaan ei luonnollisesti riitä, vaan lopputuotos sovitettava myös paikallisiin reunaehtoihin ja otettava huomioon mm. kansalliset linjaukset ja sovitettava tekeminen niiden asettamiin reunaehtoihin<br>- kartoitusvaiheessa (ts. ei kuvauksia juurikaan tehty, mutta niitä tarvittaisiin) oleville hankkeille nähtiin hyödylliseksi prioriteetti-sarakkeen lisääminen kuvauksille<br>- mallien käyttämiseen, asioiden läpikäynti ja selittäminen työpajamaisesti auttoi toteuttajaa selkeyttämään omia suunnitelmiaan<br>- läpikäydyissä malleissa ja listauksissa sekä läpikäynneissä tehdyissä muistiinpanoissa nähtiin olevan paljon suoraan hyödynnettävää pohjaa tulevassa dokumentaatiotyössä |

# 4 Yhteenveto case-läpikäynnistä ja arviointia

Seuraavaan poimittu, niin tutkijoiden kuin tietolähteinä toimineen haastateltavan näkemyksiä läpikäynnistä mm. hyödynnetyistä menetelmistä ja välineistä, kokonaisarkkitehtuurimallin hyödyntämisestä kohdealueella sekä saavutetuista tuloksista:

*Menetelmät ja läpikäynti:*

- SOLEAn tuottamissa menetelmissä ja välineissä esitettävät listaukset ja mallit voivat toimia tarkistuslistoina, mutta ovat myös vain ehdotuksina tai templaatteina, siitä mitä ratkaisukenttä sisältää. Onkin nähty oleelliseksi myös tarkastella mallien yhteydessä jääkö jotain ehdotetun mallin ulkopuolelle esim. tyypillisesti tällaisia arvoja ovat eri poikkeustapaukset ympäristössä.
- Lisäyksenä edelliseen, yleinen malli ei luonnollisesti riitä, vaan lopputuotos sovitettava myös paikallisiin vaatimuksiin ja otettava huomioon mm. kansalliset linjaukset ja sovitettava tekeminen myös niiden asettamiin reunaehtoihin.
- Useat mallit ovat hyödynnettävissä varsin suoraan esim. koko hankkeen kartoitusvaiheessa, mutta toisaalta myös usean menetelmän nähtiin menevän liian tarkalle tasolle vielä hankkeen alkuvaiheessa. Tällöin menetelmä vaatii soveltamista, esim. sillä tuotetaan muistilista vielä tarkennettavista seikoista, joihin voidaan palata projektin myöhemmissä vaiheissa asioiden tarkennuttua. Toinen hyödynnetty tapa edellä kuvatun ongelman välttämiseksi läpikäynnissä oli abstraktiotason nostaminen, esim. SOA-palvelulistaus ja -kuvaukset päätettiin hyödyntää vain niiden tarjoamien toiminnallisuuksien osalta eli listauksena: ”*mitä toiminnallisuuksia ratkaisulta vaaditaan?*”, ilman sen tarkempia teknologia yms. toteutuslinjauksia.

- Kartoitusvaiheessa oleville hankkeille, ts. ei määrityksiä, dokumentaatiota ja kuvauksia juurikaan vielä tehty, mutta niitä tarvittaisiin, nähtiin hyödylliseksi priorisoinnin/vaiheistuksen muistiinpanojen mahdollistaminen mallien oheen (esim. prioriteettisarakkeen lisääminen tms.) eri osakokonaisuuksille (esim. kuvattavien asioiden järjestys, toteutusjärjestys prosesseille tai ratkaisulle asiakas-/käyttäjäsegmenteittäin jne.)

*IDM ja kokonaisarkkitehtuuri:*

- SOLEAssa laadittu toimialue (domain) –kohtainen menetelmä- ja välinepaketti (Liite 1, luku 2) soveltui johdannoksi (ensimmäiseksi vaiheeksi) läpikäyntiin (mm. haastattelijan ja haastateltavan käyttämän käsitteistön ja näkemyksien yhteensovittamisessa) ennen menoa geneerisempiin toimialueriippumattomiin kokonaisarkkitehtuurillisiin menetelmiin (Liite 1, luku 3)
- menetelmä- ja välinepaketti sisälsi myös välineitä, joilla saatujen tuloksien kirjaaminen onnistunee suhteellisen suoraviivaisesti kokonaisarkkitehtuurikuvauspohjiin (mm. prosessit, tietojärjestelmäpalvelut, kehittämistarpeet) esim. osaksi organisaation kokonaisarkkitehtuurillista tavoitetilankuvausta (tai vastaavasti esim. käyttäjähallinnan segmenttiarkkitehtuurikuvauksia)
- tarkasteltavassa projektia SOLEAn *Arkkitehtuurin kuvaustapojen tiedonkeruu, pohjataulukkoa: 3 - Kuvausten läpikäynti tasoittain* (Liite 1, luku 3.2), joka sisältää tyypillisten kokonaisarkkitehtuurikuvauskokonaisuuden, sen avulla havaittiin, että kyseisen projektin tarvitsema kuvauskokonaisuus on sangen kattava suhteessa listaukseen ja useat vaikka vain käyttäjänhallinnan näkökulmasta tehdyt kuvaukset ovat kattavuudeltaan koko organisaation mittakaavassa (esim. sovellus-, rooli- ja toimipaikkalistaukset)
- edelliset havainnot vahvistavat tutkijoiden puolesta esitettyä näkemystä, siitä että esim. mittavat organisaationaliset kehityshankkeet, kuten tässä yhteydessä käyttäjä-/käytönhallinnan kehitysprojekti, voivat tuottaa hyötyjä myös koko organisaation arkkitehtuurin hallintaan tähtääville hankkeille (kokonaisarkkitehtuurin kehityshankkeille)
- vastaavasti myös toisinpäin: käyttäjä-/käytönhallinta-hanke voi hyödyntää useita kokonaisarkkitehtuurin elementtejä pohjina tai sellaisenaan ja joka tapauksessa molemmilla kehityspanostuksille on nähtävissä synergiaetuja keskinäisestä tiedonvaihdosta ja yhteistyöstä
- läpikäyntien aikana nähtiin hahmottuvan myös arkkitehtuuriperiaatetasolle meneviä yleisiä malleja, kuten yhtenäinen rooli-malli järjestelmille sekä yhtenäinen liittämismalli yksittäisille järjestelmille käyttäjähallintajärjestelmän piiriin
- haastateltavan tai tilaajan organisaatiossa ei vielä haastattelun tekoaikana ollut käynnissä kokonaisarkkitehtuurin kehittämishanketta, mutta meneillään olevan käyttäjä-/käytönhallinnan projektin nähtiin voivan toimia hyvänä lähtölaukauksena kyseiselle työlle tai vähintään olevan hyödynnettävissä siinä

*Saadut tulokset:*

- mallien käyttämiseen sekä asioiden läpikäynti ja selittäminen työpajamaisesti auttoi toteuttajaa selkeyttämään omia suunnitelmiaan

- haastateltavan vetämän projektin läpikäynti tutkimushankkeessa tuotetuin usein eri menetelmin, pääasiassa tarkastuslista tyyppisesti, tuotti alkuvaiheessa olevalle projektille sisältöjen ja suunniteltujen kokonaisuuksien suhteen täydennystä (mm. tarvittavat kuvaukset -lista) sekä ilmenneille työkohteille useita alustavia priorisointi-/vaiheistuslistauksia
- em. liittyen esiin nousseita ja läpikäyntien aikana saatuja tarkennuksia, linjauksia ja rajauksia on jo hyödynnetty kehityshankkeen dokumentaatiossa (sekä myös SOLEA:n aihealueelle tässä dokumentissa tuottamaa näkemystä kohdealueesta, mm. käsitteistö nähtiin hyödynnettäväksi sellaisenaan) ja nähtiin jatkossa hyödynnettäviksi myös lisää
- läpikäynneissä työstettyä materiaalia hyödynnetään tukimateriaalina myös kommunikoinnissa liiketoimintatasolle ja em. hankintapäätöksen hakemisessa, tämä kuitenkin vaatii vielä materiaalin räätälöimistä myös liiketoiminta-tasolle viestintään soveltuvaksi.
- tutkimusosapuolelle tuotettujen mallien hyödyntäminen käytännön projektin yhteydessä auttoi mm. menetelmien ja välineiden kattavuustarkastelussa, täydentämään välineitä sekä kehittämään välineistön hyödyntämismalleja.