Kuntasektorin arkkitehtuuriryhmä

Kuntasektorin käyttövaltuushallinnan viitearkkitehtuuri

Versio 1.0

Viitearkkitehtuurin kuvaus

Helsinki 2013
ISBN 978-952-384-3

Kuntaliitto
Kommunförbundet

Sisältö

1 Johdanto

Tämä viitearkkitehtuuri on tarkoitettu käytettäväksi ohjeena ratkaisua kuvattaessa ja toteutettaessa. Tavoitteena on käyttövaltuushallinnan prosessien ja käsitteiden yhdenmukaisuus ja toteutusratkaisujen yhteentoimivuus. Viitearkkitehtuurin avulla yksittäisen kunnan on helppo ottaa käyttöön kuntien tai kunnan yhteinen tai yhteensopiva käyttövaltuuksien hallinta.

Viitearkkitehtuuri ei siis ole yksittäisen kunnan käyttövaltuushallinnan ratkaisuarkkitehtuurikuvaus vaan tätä kuvausta voidaan käyttää pohjana kunnissa erikseen määritettävälle ratkaisuarkkitehtuurille ja toteutukselle.

Viitearkkitehtuurin määritelmä julkisen hallinnon Juhta suosituksen JHS 159 mukaan on:
Viitearkkitehtuuri on rajatun arkkitehtuurikokonaisuuden abstrakti toimittaja- ja toteutusneutraali rakenne. Se on esitys arkkitehtuurikokonaisuuden loogisista osista ja niiden välisistä suhteista. Viitearkkitehtuurilla ohjataan arkkitehtuurisuunnittelua halutunlaiseen toteutusrakenteeseen. Viitearkkitehtuuri voi olla organisaation sisäinen, toimialaan liittyvä tai yleinen looginen rakennemalli.

Viitearkkitehtuuri on toteutusneutraali lainsäädännön vaatimukset täyttävä arkkitehtuurikehys, jonka puitteissa eri viranomaiset/asianosaiset voivat toteuttaa järjestelmän toimialasta riippumatta.

Viitearkkitehtuurikuvauskokonaisuus koostuu tästä päädokumentista - viitearkkitehtuurikuvauksesta sekä viidestä liitteestä, jotka tarkentavat tätä kuvausta. Jos haluaa perehtyä vain yleisellä tasolla käyttövaltuushallinta kokonaisuuteen, suositellaan luettavaksi tämän dokumentin kohdat:

- Arkkitehtuurin yleiskuvaus, luku 7
- Käyttövaltuushallinnan prosessikuvaukset ja toimintalogiikka, luku 8

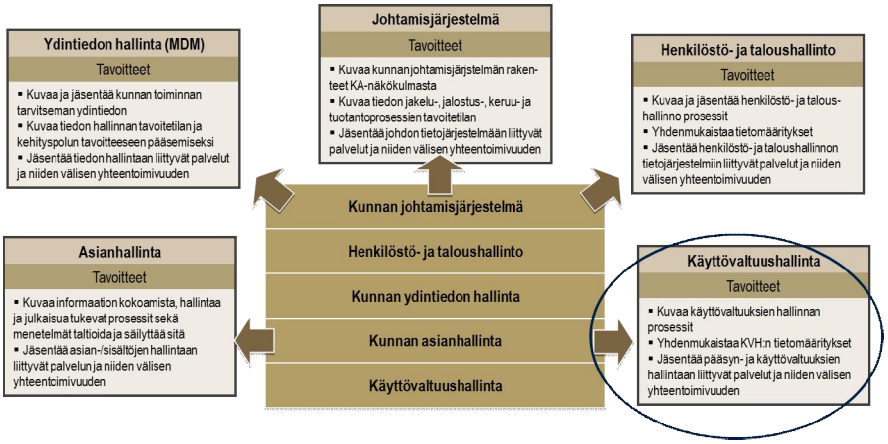
2 Taustaa

2.1 Käyttövaltuushallinnan lähtökohdat

Tämä dokumentti on esitys Kuntasektorin yhteinen kokonaisarkkitehtuuri – hankkeen yhden osa-alueen – käyttövaltuushallinta- viitearkkitehtuuriprojektin käynnistämiseksi. Projektin lähtökohtana on Kuntaliiton, JulkICT:n (aikaisemmin KuntaIT) ja kuntien arkkitehtuuriryhmän kesäkuussa 2011 pitämä Kurttu-seminaari ja sen työryhmien

tuotokset sekä maaliskuussa 2012 pidetty Kurttu-seminaari ja sen työpajojen tuotokset.

Kurttu-seminaareissa on tunnistettu seuraavat kuntasektorin yhteiset viitearkkitehtuurit (tässä viitearkkitehtuurissa kuvattu kokonaisuus):



Kuva 1: Kuntasektorin yhteisestä kokonaisarkkitehtuurista tässä kuvattava kokonaisuus: Käyttövaltuushallinta – viitearkkitehtuuri.

2.2 Projektointi

Tämä kuvaus on laadittu yhteistyössä Kuntaliiton, Valtiovarainministeriön ja eri kuntien sekä HUS:n kanssa.

Viitearkkitehtuuri-projektin toteutusvaiheen hyväksyntä ja käynnistäminen:

- Kuntaliitto päätti projektin käynnistämisestä, asettamisesta
- Projektin ohjaukseen liittyvästä päätöksenteosta vastaa Kuntasektorin KA- ohjausryhmä.
- VM rahoittaa projektia omalta osaltaan. Projektin käynnistämisvaatimuksena oli VM:n myönteinen rahoituspäätös projektin toteutuksesta.

Projekti ja ohjausryhmät olivat:

Kuvaus on osa kuntasektorin kokonaisarkkitehtuurityötä ja sitä hallinnoidaan ja ylläpidetään kuntasektorin kokonaisarkkitehtuurin (KA) hallintamallin prosessien mukaisesti. Kuvauksen vastuullinen omistaja/ hallinnoija on Kuntaliitto.

3 Kokonaisarkkitehtuurin näkökulmat

Tässä huomioitavat kokonaisarkkitehtuurinäkökulmat ovat:

Toiminnan näkökulma

- Kuvataan käyttövaltuushallinnan vaikutukset organisaation toimintamalliin. Kuvataan toimintamalli prosesseina ja esimerkkiskenaarioina.

Tietojen näkökulma

- Kuvataan käyttövaltuushallintaan liittyvät käsitteet ja käsitteiden väliset suhteet ja tiettyjen käsitteiden osalta tietomalli. Kuvataan kohdealueen sanasto. Sanasto on erillinen liite.

Tietojärjestelmä-näkökulma

- Tietojärjestelmä-näkökulmasta kuvataan kohdealueeseen liittyvät järjestelmät loogisella tasolla, ns. ympäristökuvaus ja järjestelmien välinen tietovirtakuvaus.

Teknologia-näkökulma

- Teknologia-näkökulmasta otetaan kantaa julkisessa hallinnossa määriteltyihin ja noudatettaviin suosituksiin, jotka liittyvät standardeihin. Tarkempaa teknologiakuvausta ei tässä dokumentaatiossa tehdä.

4 Viitearkkitehtuurin muutosten hallinta

Viitearkkitehtuurin hyväksymisen jälkeen tulevat muutokset ja arkkitehtuurin lisäykset tai tarkennukset hallitaan kuntasektorin KA-hallintamallin mukaisesti. Kuntasektorin KA-hallintamallissa on kuvattu muutoshallintaprosessi, jonka mukaisen käsittely-, päätösvaiheiden ja aikataulun mukaan päivitykset viedään viitearkkitehtuuriin. Kuntasektorin hallintamalli löytyy kuntaliiton sivuilta ja kuntaportaalista.

5 Arkkitehtuurin hyödyt ja soveltaminen

Viitearkkitehtuurin toteuttaminen aiheuttaa kustannuksia organisaatiolle. Kustannusten vastineeksi organisaatio saa hyötyä viitearkkitehtuurin mukaisesta toteutuksesta ja käyttövaltuuksien automatisoinnista. Palvelun yhdenmukainen toteutustapa tai jopa yhteinen palvelu lisää toiminnan tehokkuutta ja tietojen sekä palvelujen yhteiskäyttöisyyttä luottamusverkon sisällä.

Hyötyjen konkretisointi ja mittaaminen on usein vaikeaa. Käyttövaltuushallinnan piirissä olevien palvelujen käyttäjien saama todellinen hyöty tai kokema hyöty on edellytys koko organisaation hyötyjen toteutumiselle. Hyötyjä tulisi arvioida toiminnan tehostumisen ja palvelujen käyttäjien kokeman hyödyn näkökulmasta

5.1 Hyödyt

Hyötyjä tarkastellaan käyttövaltuushallinnan kahden osakokonaisuuden näkökulmasta. Ks. Kuva 3: Käyttövaltuushallinnan osakokonaisuudet

5.1.1 KVH (IAM) hyödyt

Keskitetty käyttövaltuushallinta on kustannustehokasta. Käyttövaltuushallinta automatisoi useita työläitä ja resursseja kuluttavia tehtäviä sekä systematisoi käyttäjien valtuutusten sekä palveluiden ja järjestelmien käyttöoikeuksien hallinnan.

Käyttövaltuushallinnasta saatavia konkreettisia hyötyjä:

- Voidaan parantaa sovellusten tietoturvatasoa ilman että sovellusta tarvitsee muuttaa.
- Tiedetään kenellä on tai on ollut oikeus käyttää tietojärjestelmiä.
- Vähennetään väärinkäytösten mahdollisuutta.
- Mahdollistetaan keskitetty pääsynhallinta.
- Nopeutetaan luvitusprosesseja: nopeutetaan sovellusten käyttöönottoja yhtenäisen toiminta- ja tietomallin avulla.
- Vähennetään esimiesten, helpdeskin ja sovellusvastuuhenkilöiden työtä.
- Toteutetaan lain vaatimukset mm. yksityisyydensuojan ja henkilötietolain osalta.
- Mahdollistetaan auditointikelpoinen käyttöoikeushallinta: mahdollistetaan mm. viransijaisuuksien hallittu ja auditoitavissa oleva hoitaminen.
- Voidaan hyödyntää yhteistä korkean käytettävyyden ympäristöä.
- Saadaan neuvotteluvoimaa sovelluspalveluiden tuottajille.
- Voidaan hyödyntää parhaita yhteisiä prosessimalleja.

5.1.2 Kertakirjautumispalvelun hyödyt

Kertakirjautumisen palvelun seurauksena saavutetaan heti konkreettisia, nopeasti saavutettavia hyötyjä, joita ovat mm. seuraavat:

- Keskitetty käyttäjätunnusten hallinta on kustannustehokasta; automatisoinnin perusteella työn määrä vähenee ja hallinta nopeutuu.
- Virheistä aiheutuvien tikettien määrä vähenee; keskitetty automaattinen hallinta noudattaa ennalta määriteltyä ja testattua prosessia, jolloin inhimillisten virheiden määrä vähenee.
- Käyttäjätyytyväisyys kasvaa; Asiakkaiden, kumppanien ja kunnan toimijoiden työn tekeminen ja asiointi helpottuu ja nopeutuu, kun ei tarvitse muistaa lukuisia tunnuksia => työn tuottavuus kasvaa.
- Tietoturvallisuus kasvaa; Käyttäjät ja asiakkaat tarvitsevat vain yhdet tunnukset, joiden perusteella identiteetti tunnistetaan. Ei erillisiä muistilappuja lukuisista tunnuksista.
- Salasanojen unohtumisesta johtuvat katkot työn suorittamisessa vähenevät ja salasanojen resetointi vähenee.

5.2 Viitearkkitehtuurin soveltamisohjeita

Kunnilla on erilaisia tarpeita toteuttaa käyttövaltuushallintaa. Lähtötilanne ja kyvykkyys käyttövaltuuksien hallintaan määrittelevät, mistä lähdetään liikkeelle ja miten viitearkkitehtuurikokonaisuutta sovitetaan kunnan toimintaympäristöön. Toteutuksella tulee olla johdon tuki ja strateginen linjaus toteutettavasta toimintaympäristöstä. Esimerkiksi eri kunnilla saattaa olla eri tasoiset vaatimukset tunnistuksen osalta: jotkut kunnat vaativat aina TUPAS/VETUMA-tunnistusta, toiset kunnat käyttävät TU-

PAS/VETUMA-tunnistusta ensimmäisellä käyttökerralla ja haluavat käyttää käyttäjätunnus ja salasana -tunnistusta seuraavilla kerroilla.

Esimerkiksi erilaisia tarpeita voivat olla:

- Käyttäjätunnistus tarvitaan työntekijöille ja luottamushenkilöille sekä kuntalaisille.
- Kertakirjautuminen tarvitaan kaikille käyttäjäryhmille.
- Kertakirjautumisen tulisi kattaa kunnan lisäksi myös muut julkishallinnon toimijat (Verottaja, Kela jne.).
- Kertakirjautumisen piiriin pitää saada myös kolmansien osapuolien tuottamat sovellukset tai kolmansien osapuolien tarjoamat palvelut (koulutoimessa Helmi / Wilma, kirjastojen web-sovellukset jne.), joilla kaikilla on nykyisin omat käyttöoikeushakemistonsa.
- Käyttöoikeushallinta halutaan niille käyttäjäryhmille, joille sitä tarvitaan.
- Kunnan työntekijät tarvitsevat tarkkaa roolipohjaista käyttövaltuushallintaa, jotta terveyteen ja toimeentuloon jne. liittyviä tietoja ei näy asiaankuulumattomille.
- Kunnan ”edustajana” ja ”sisäisenä” sovelluksen käyttäjänä voi toimia kunnan omien työntekijöiden lisäksi myös joku ulkopuolinen taho, kuten päivähoitoa tai vanhusten hoitopalvelua tuottava kaupallinen toimija tai ulkoistettu asiakaspalvelu.
- Käyttöoikeushallinta tarvitaan kaikille kunnan työntekijöille.
- jne.

Viitearkkitehtuuri ohjaa toteutusta yhteentoimivuuden lisäämiseksi. Viitearkkitehtuurin huomioiminen toteutusratkaisussa mahdollistaa yhteisten palvelujen käytön sekä mahdollisesti myöhemmin toteutettavan laajemman luottamusverkoston käyttöönoton. Mallin perusratkaisujen ja prosessien huomioon ottaminen käyttövaltuushallintaa suunniteltaessa tuo kustannussäästöjä, koska osa huomioitavasta ongelmakentästä on kuvattu tässä dokumentissa.

Ratkaisun hankinnan yhteydessä viitearkkitehtuuri toimii hyvänä vaatimusmäärittelykuvauksena, vaikka toteutus koskisi vain osaa viitearkkitehtuurin osa-alueista. Jos hankinnassa otetaan huomioon viitearkkitehtuuri kokonaisuutena, mahdollistetaan myöhemmin toteutettavien osien integroitavuus ja yhteentoimivuus.

Ratkaisuissa, joissa kunnilla on jo omia ratkaisuja ja infrastruktuuria, tulee analysoida miten ne voidaan hyödyntää viitearkkitehtuuri mallin soveltamisessa ja miltä osin tarvittaessa tulee tehdä muutoksia.

Käyttövaltuushallintaan liittyviä yleisiä laadullisia vaatimuksia

- Käyttäjäpotentiaali on varsin suuri; kuntien kaikki asukkaat – tulevaisuudessa. Todellista määrää on vaikea arvioida. (sähköinen asiointi)
- Työntekijöistä (sisäiset ja ulkoiset) suurin osa käyttää palveluita tavoitetilassa (sähköinen työpöytä jne.).
- Yhtäaikaisten käyttäjien määrä vaihtelee merkittävästi palveluittain ja kalenteriajallisesti. Jotkut palvelut voivat olla suhteellisen tasaisella kuormalla koko vuo-

den, toisissa palveluissa on taas hyvin suuria piikkejä esim. hakemuksen viimeisenä jättöpäivänä (Terveydenhoidossa tulee uusia hakemuksia hyvin runsaasti vuosittain)

- Hankittavan KVH-järjestelmän suunnittelussa ja hankinnassa otetaan huomioon federaatiot (tunnistuslähteen perustaminen Virtu-luottamusverkostoon (Virtu /SAML 2), tavoitteiden mukaisesti) ja luottamusverkostojen mahdollisuudet.

6 Viitearkkitehtuuriin liittyvät sidosarkkitehtuurit ja muu ohjeisto

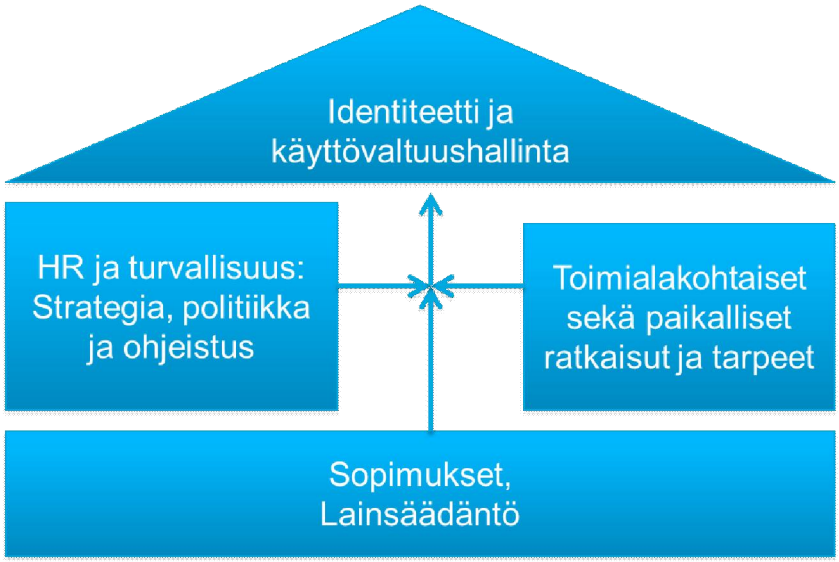
Tämän viitearkkitehtuurityön pohjalla ovat seuraavat ohjeet ja sidosarkkitehtuurikuvaukset, jotka liittyvät kohdealueeseen:

Ohje/Kuvaus	Selite/ Linkki
VAHTI 9/2006:	Käyttövaltuushallinnan periaatteet ja hyvä käytännöt http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061122Kaeyttoe/vahti_9_06.pdf
VAHTI 2/ 2012:	Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta https://www.vahtiohje.fi/c/document_library/get_file?uuid=b4a90e50-7307-4004-ac8e-b9103220db6a&groupId=10128&groupId=10229
Virtu	Virkamiehen tunnistamisen luottamusverkosto Virtu on valtionhallinnon yhteinen palvelu. Sitä käytetään organisaatiorajojen ylitse tapahtuvaan käyttäjätunnistukseen valtionhallinnon yhteisiin palveluihin Virtu-ohjeita: http://www.csc.fi/sivut/virtu
VirtuK	Kuntien käyttövaltuushallinnon kehittäminen Käyttövaltuushallinnan totutuksen suunnitelma, 2009 Ohje työntekijän tunnistamisen toteuttamisesta kunnallishallinnossa, 2009 http://wiki.kuntait.fi/tiki-index.php?page=VIRTUK
Sosiaalialan teknologiahanke	Sosiaalihuollon käyttövaltuuksien hallinta ja käytön seuranta http://www.sosiaaliportti.fi/File/9f116cda-bc29-49a8-812b-468aca8aa2cf/K%C3%A4ytt%C3%B6valtuuksien+hallinta+ja+seuranta+sosiaalihuollossa.pdf
VAHTI 3/2009	Lokiohje http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20090511Lokioh/Vahti_3_NETTI.pdf
SAML 2.0 (Security Assertions Markup Languages)	Julkisen hallinnon yhteinen SAML 2.0 profiili (SAML 2.0 protocol deployment profile) – kertakirjautumisen, valtuutusten jakamisen standardoitu viitekehys www.csc.fi/sivut/virtu/tekniikka/ http://www.csc.fi/sivut/virtu/tekniikka/maaritykset
Virtu attribuutti määritys	Virtu-käyttäjätunnistusjärjestelmän tekniset määritykset http://www.csc.fi/sivut/virtu/tekniikka/maaritykset

Vetuma	JHS 164 Tunnistautuminen ja maksaminen sähköisessä asioinnissa VETUMA-palvelun avulla JHS 164 http://www.jhs-suositukset.fi/suomi/jhs164
Hakemistotiedot ja niiden ylläpito	JHS 133 Hakemistotiedot ja niiden ylläpito http://www.jhs-suositukset.fi/web/guest/jhs/recommendations/133
Rekisteriseloste	Henkilötietolaissa määritelty asiakirja, joka jokaisen rekisterinpitäjän on laadittava ja pidettävä jokaisen saatavilla. Lomake : http://www.tietosuoja.fi/
Kuntasektorin KA-hallintamalli	Kuntasektorin kokonaisarkkitehtuurin hallintamalli
Haka luottamusverkko	Yliopistojen, korkeakoulujen ja tutkimuslaitosten sekä näitä palvelevien yhteisöjen luottamusverkko http://www.csc.fi/hallinto/haka

7 Arkkitehtuurin yleiskuvaus

Käyttövaltuushallinnan viitearkkitehtuurissa otetaan huomioon eri lähtökohdat ja olemassa oleva lähdemateriaali. Viitearkkitehtuurissa tarkastellaan käyttövaltuushallintaa kokonaisuutena, jossa henkilöstöhallinnon prosessit ja järjestelmät ovat keskeisessä asemassa. Toimialakohtaiset ja paikalliset ratkaisut sekä tarpeet tulee ottaa huomioon käyttövaltuuksien hallintaa suunniteltaessa ja toteutettaessa. Viitearkkitehtuurissa kuvataan käyttäjien identiteetin ja valtuutusten hallintaa laajemmin sekä kunnan että koko kunnan toimintaympäristön näkökulmasta ja tarpeista, mukaan lukien luottamusverkkohierarkian hallinta.



Kuva 2: Käyttövaltuuksien hallinnan lähtökohdat

Käyttövaltuushallinta on olennainen osa toimintaa ja se tukee toimintaan liittyvän lainsäädännön toteutumista sekä huomioi paikalliset ratkaisut ja tarpeet.

Kuva 3: Käyttövaltuushallinnan osakokonaisuudet toteutuksen tarkastelunäkökulmasta

Käyttövaltuushallinta- (IAM – Identity and Access Management)) on sateenvarjokäsite, joka muodostuu karkealla jaottelulla toteutuksen näkökulmasta kahdesta osakokonaisuudesta. Osakokonaisuudet ovat toteutettavissa vaiheittain

Kertakirjautuminen

- Koko organisaation laajuinen kertakirjautumisen ratkaisu, joka kattaa kokonaan tai lähes kokonaan organisaation tietojärjestelmäpalvelut.
- Kertakirjautuminen on kokonaisuuden kannalta itsenäinen palvelu, joka voidaan toteuttaa omana kokonaisuutena.

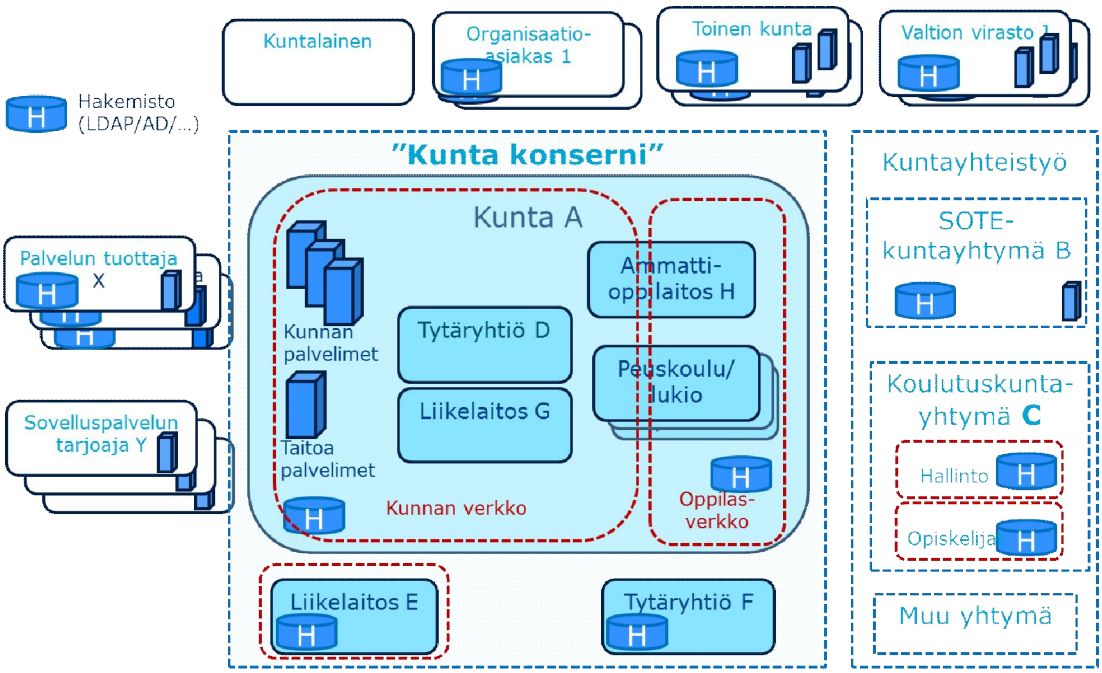
Identiteetin ja käyttövaltuuksien hallinta

- Pääsyn-, käyttäjävaltuuksien sekä identiteettien hallinta.

Tässä dokumentissa tarkoitetaan käyttövaltuus- ja identiteetinhallinnalla seuraavia tarkemman tason kokonaisuuksia, jotka on kuvattu tarkemmin kappaleessa Järjestelmäarkkitehtuuri loogisella tasolla

- Identiteetin hallinta
- Käyttäjä- ja käyttövaltuushakemisto
- Kertakirjautuminen
- Vahva tunnistus
- Web-pääsynhallinta
- Federoitu pääsynhallinta
- Suostumusten ja valtuutuksien hallinta
- Palveluiden ja integraatioiden pääsynhallinta
- Ulkoinen käyttöoikeuksien päättely

Kunnan nykyinen toimintaympäristö ja tavoitetilan toimintaympäristö sanelevat, miten käyttövaltuushallintaa kehitetään ja mitkä ovat ne olemassa olevat osat, jotka tulee ottaa huomioon. Alla on kuvattu esimerkinomaisesti kunnan toimintaympäristön kokonaiskuva, joka toimii lähtökohtana käyttövaltuushallintaa ja luottamusverkkoa suunniteltaessa.



Kuva 4: Esimerkki_kunnan toimintaympäristöstä, kokonaiskuva

Viitearkkitehtuurissa tarkastellaan kuntia ja muita kuntatoimijoita sekä niiden toimintaympäristöä käyttäjä- ja käyttöoikeushallinnan sekä pääsynvalvonnan näkökulmasta. Myös tästä näkökulmasta tarkasteltuna kunnat ja niiden toimintaympäristöt ovat varsin erilaisia.

Keskeisimpiä tarkastelukohteita ovat:

- Yhteistyökumppanit
  - Laajemmat hallinnolliset yhteistyökumppanuudet, esimerkiksi SOTE -kuntayhtymä, jossa on sekä perusterveydenhuollon että erikoissairaanhoidon tarkastelunäkökulmat tai koulutuskuntayhtymät, jne.
  - Yhteisten palvelujen/ sovelluspalvelujen toteuttamisen kautta syntyvä yhteistyö esimerkiksi eri kuntien kesken
  - Yhteisten palvelujen/sovelluspalvelujen hyödyntämisen kautta syntyvä yhteistyö esimerkiksi valtion virastojen kanssa
- Palvelun tuottajat, ulkoiset ostopalveluiden tuottajat, jotka tarjoavat palvelujaan kunnalle
- Sovelluspalveluiden tarjoajat, ulkoiset ostettavat tai tuotettavat sovelluspalvelut, pilvipalvelut, joita kunnassa hyödynnetään
- Asiakkaat, sekä kuntalaiset että yritysasiakkaat palvelujen hyödyntämisen näkökulmasta

Kunnilla on tyypillisesti oma käyttöoikeusverkkonsa tai useita käyttöoikeusverkkoja. Kunnan käyttöoikeusverkko voi olla kunnan itsensä ylläpitämä tai jonkun palveluntarjoajan tuottama. Esimerkkikuvassa on piirretty kunnan hallinnollinen verkko ja erillinen oppilasverkko. Kunnan liikelaitokset ja tytäryhtiöt voivat toimia kunnan verkossa tai niillä voi olla omat verkkonsa. Samoin esimerkiksi SOTE- ja sivistystoimen organi-

saatiot voivat toimia osana kunnan verkkoa tai niillä voi olla omat verkkonsa. Erilaisia kombinaatioita on suuri määrä.
Yleisesti verkolla tässä tarkoitetaan loogisia käyttövaltuusalueita.

Kunnan työntekijät voivat tarvita työssään myös valtion virastojen tai muiden julkisen sektorin toimijoiden tarjoamia sovelluspalveluita. Kunnat voivat tarjota vastavuoroisesti pääsyn sovelluspalveluihinsa muille julkisen sektorin toimijoille.
Kuntien käyttämät sovelluspalvelut voidaan tuottaa kuntien omissa verkoissa tai ulkoisen sovelluspalveluntarjoajan verkossa. Erilaisia tapoja ottaa yhteys tarjottuun palveluun ovat mm. verkot yhdistävä VPN-putki, internetin yli käytettävät web-käyttöliittymät tai virtualisoidut työpöydät jne.

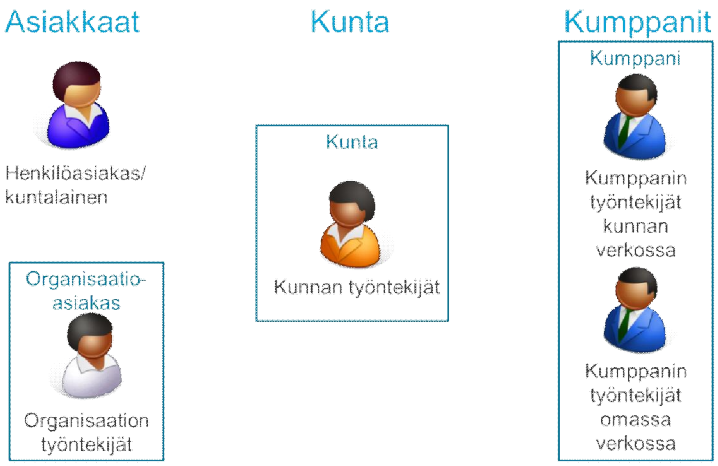
Kunnan toimintaympäristö on lähtökohtana kunnan luottamusverkon määrittelyyn ja siihen pohjautuvien hierarkkisuusehtojen määrittelyyn.

8 Käyttövaltuushallinnan prosessikuvaukset ja toimintalogiikka

8.1 Käyttäjät /Roolit ylätasolla

Karkealla tasolla kunta ja sen ympärillä toimivat tahot ja käyttäjät (kuva alla) voidaan jakaa seuraaviin ryhmiin:

1. Asiakkaat:
   - henkilöasiakkaat (myös henkilön puolesta asioivat)
   - organisaatioasiakkaat/organisaationasiakkaan työntekijät
2. Kunta
   - kunnan sisäiset työntekijät
3. Kumppanit
   - kumppanin työntekijät kunnan verkossa
   - kumppanin työntekijät omassa verkossaan



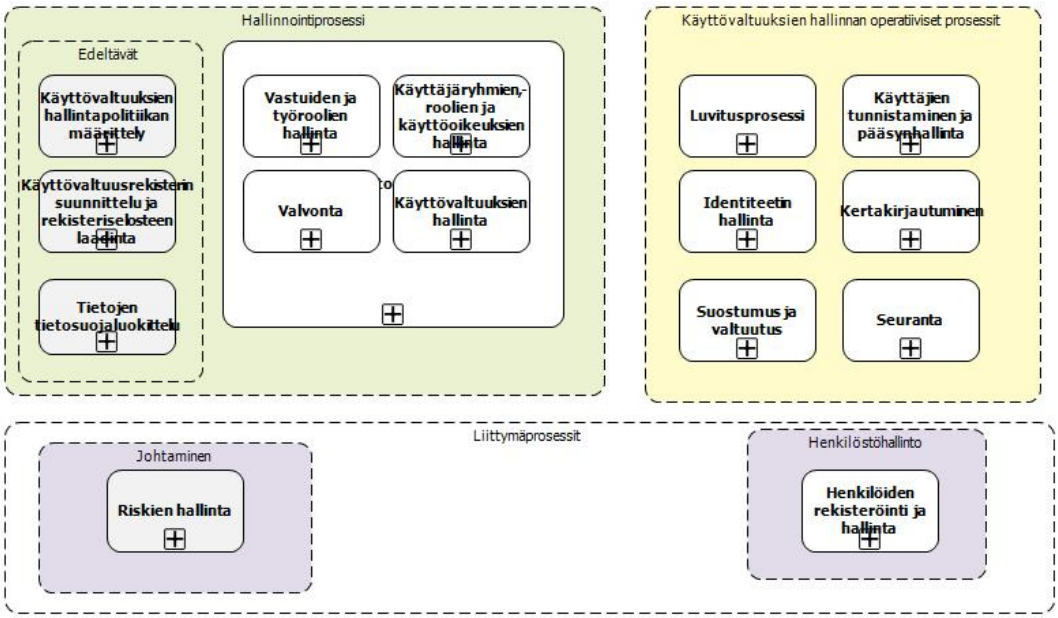
Kuva 5: Kunnan ympärillä toimivat käyttäjät karkeasti ryhmiteltynä.

Ryhmä	Käyttäjä	Kuvaus
Asiakkaat	Henkilöasiakas	Kunnan kanssa asioiva tai asioita hoitava/puolesta asioiva henkilö: • kuntalainen • ei-kuntalainen • jne.
	Organisaatioasiakas	Kunnan kanssa asioiva tai asioita hoitavan organisaation työntekijä tai jäsen. Organisaatioita voivat olla esimerkiksi • urheiluseurat • rakennusliikkeet • muut yritykset tai yhdistykset
Kunta	Kunnan työntekijä	Kunnan työntekijä: • kunnan virkamies • työsuhteinen työtekijä • jne.
	Muu kunnan toimija	Kunnan muu edustaja: • luottamushenkilö tms. Kunnan käyttöoikeusverkkoa hyödyntävän organisaation työntekijät tai jäsenet: • oppilas • tytäryhtiön työntekijä • jne.
Kumppanit	Kumppanin työntekijä kunnan verkossa	Kunnalle tai kunnan puolesta palveluita tarjoavan/tuottavan organisaation työntekijä tai jäsen, joka käyttää näiden tehtävien hoitamiseen kunnan käyttöoikeusverkkoa. Esimerkiksi: • vuokratyövoima • keikkalääkäri • räätälisovelluksen kehittäjä Tällainen kumppanin työntekijä hyödyntää usein runsaasti kunnan tarjoamia tietojärjestelmäpal-

		veluita.
	Kumppanin työntekijä omassa verkossaan	Kunnalle tai kunnan puolesta palveluita tarjoavan/tuottavan organisaation työntekijä/jäsen, joka käyttää näiden tehtävien hoitamiseen pääasiassa oman organisaationsa käyttöoikeusverkkoa. Tällaisia kumppaneita voivat olla esimerkiksi • yksityinen päiväkoti • yleishyödyllisen organisaation hoitokoti • ruokapalveluita tuotava yritys • tietojärjestelmätoimittajan pääkäyttäjä Tällainen kumppanin työntekijä hyödyntää yleensä kunnan tarjoamia tietojärjestelmäpalveluita vain vähäisessä määrin.

8.2 Prosessikartta

Tässä viitearkkitehtuurissa käyttövaltuushallintaa tarkastellaan kahtena osakokonaisuutena: hallinnointiprosesseina ja operatiivisina prosesseina. Hallinnointiprosessi jakaantuu tarkasteltaviin käyttövaltuushallinnan perusprosesseihin ja niitä edeltäviin prosesseihin tai vaatimuksiin, joiden pitää olla tehtynä onnistuneen käyttövaltuushallinnan käyttöönotossa.



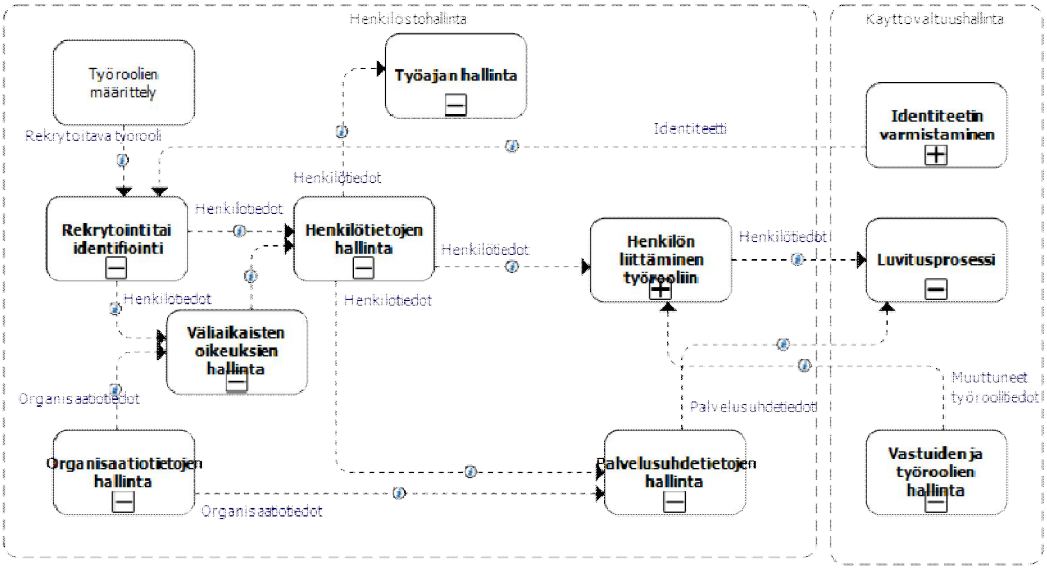
Kuva 6: Käyttövaltuushallinnan prosessikartta

Käyttövaltuushallinnan prosessit ovat kiinteässä yhteistyössä henkilöstöhallinnan prosessien kanssa. Käyttövaltuushallinta alkaa henkilöstöhallinnon prosesseista ja päättyy normaalissa työsuhteessa työsuhteen ja palkanmaksun päätyttyä.

Käyttövaltuushallinnan prosesseja tarkastellaan toiminnan näkökulmasta, ei teknisten ratkaisujen tai tuotteidentuotepakettien/palveluiden näkökulmasta

8.3 Henkilöstöhallinnan prosessien yhteys käyttövaltuushallintaan

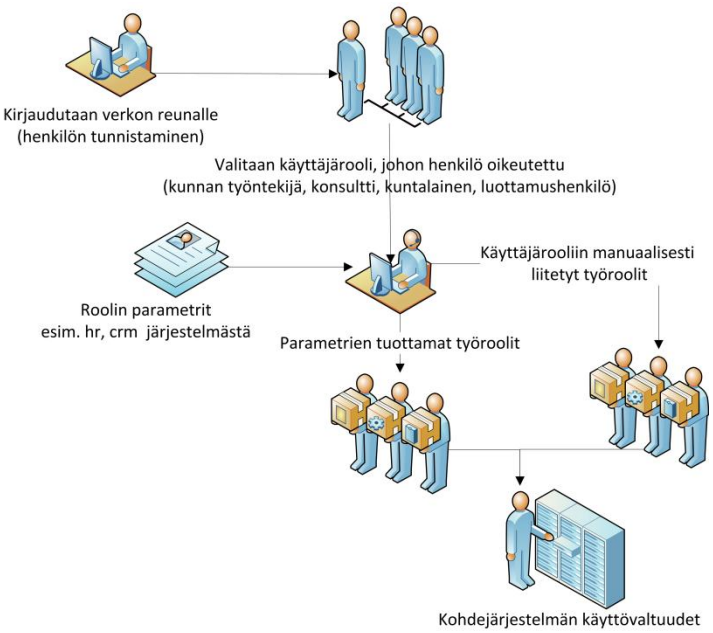
Henkilöstöhallinnan prosessit ja käyttövaltuushallinnan prosessit linkittyvät tiiviisti keskenään. Käyttövaltuuksien hallinta alkaa henkilöstöhallinnan puolelta uuden työntekijän kirjoitettua työsopimuksen tai jo ennen sopimuksen allekirjoitusta rekrytointiprosessin aikana. Viitearkkitehtuurissa on kuvattu ne tehtävät, joita henkilöstöhallinnon prosessien edellytetään tekevän, jotta käyttövaltuuksien hallinta voisi onnistua (katso kuva alla).



Kuva 7: Henkilöstöhallinnan ja käyttövaltuushallinnan välinen tietovirta

Työroolit

Henkilö tulee kiinnittää työrooleihin henkilön perustietojen luomisen yhteydessä. Rekrytoinnin yhteydessä määritellään mihin työrooliin tai työrooleihin henkilöä haetaan, joten työrooliin kiinnittäminen tapahtuu siinä yhteydessä. Henkilöön voidaan liittää useita työrooleja. Henkilön, jolla on useita työrooleja tulee valita tunnistautumisen yhteydessä mikä on työrooli, jolla haluaa toimia. (katso kuva alla)



Kuva 7b. Työroolin valinta

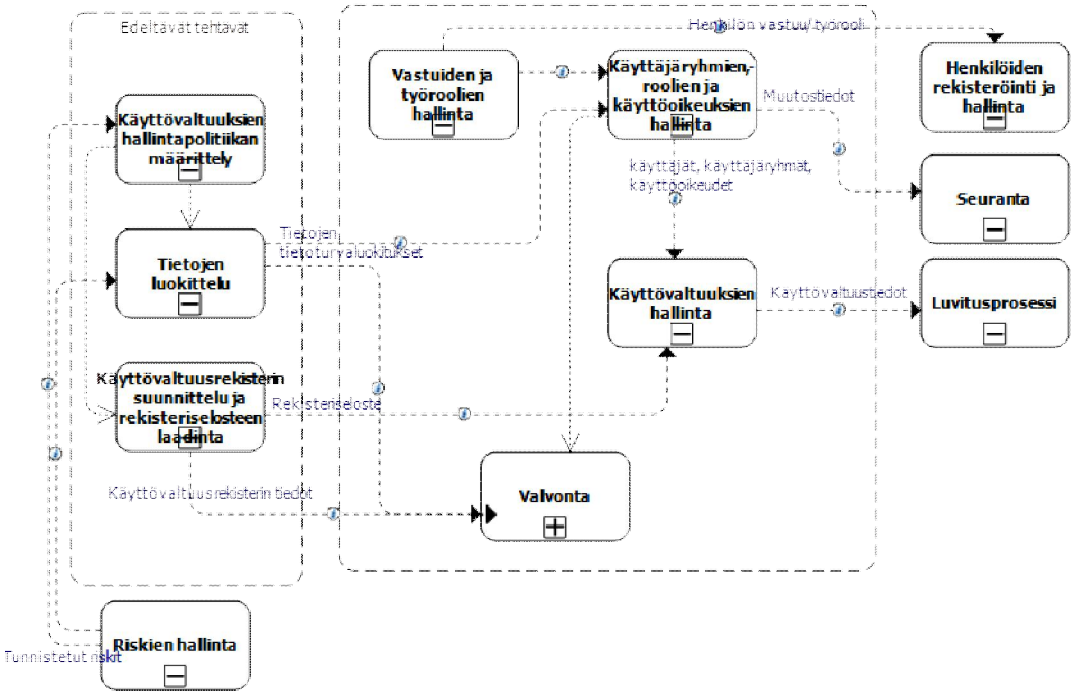
Käyttövaltuustietojen hallitsemiseksi luodaan organisaation yhteinen työroolisto. Työrooleille on nimettävä omistaja. Henkilöstöhallinnon nimeämä vastuuhenkilö ylläpitää vastaavuustaulukkoa työroolien ja lähdejärjestelmien välillä. Työroolit ovat käyttövaltuushallinnan lähtökohta. Työroolien määrään on suhtauduttava kriittisesti. Hallinta on mahdotonta, jos työrooleja on satoja, joten tavoitteena tulisi olla noin sata roolia tai alle sen. Työroolit eivät ole henkilöstöhallinnon hallinnoimia tehtävänkuvia, vaan käyttövaltuushallinnan tarvitsemia rooleja käyttövaltuuksien hallinnoimiseksi. Työroolit voidaan johtaa, koota tai purkaa Henkilöstöhallinnon tehtävänkuvista. Työrooleihin voi liittyä tarkentavia attribuutteja, esimerkiksi sijainti, joka vaikuttaa käyttöoikeuksiin. Työroolit pitävät sisällään myös asiakkaiden eli palvelujen käyttäjien roolituksen ja tämän perusteella valtuuksien määrittelyn.

Henkilöt rekisteröidään usein jo ennen työsuhteen alkua, kun esimies tekee alustavan työsopimuksen. Alustava tai ennakoiva rekisteröinti tehdään kunnan käytännön mukaan rekrytointiohjelmaan, henkilöstöhallintaohjelmaan tai siihen liitettyyn erilliseen järjestelmään.

Prosessi/tehtävä	Kuvaus	Tiedot/tulos
Työroolien määrittely ja ylläpito: (Business role)	Määritellään ja ylläpidetään organisaation yleiset työroolit, jota käytetään henkilön työtehtäviä kuvaamaan.	Työroolit
Rekrytointi/ identifiointi	Henkilöiden ja toimijoiden rekrytointi ja identifiointi: • Sisäisen työntekijän identifiointi kunnan työntekijäksi: määritellään työrooli, johon henkilöä haetaan	Rekrytoitava työrooli

	• Ulkopuolisen toimijan tai yhteistyökumppanin identifiointi kunnan toimijaksi: henkilöstöhallintoon on pystyttävä lisäämään myös ulkopuoliset toimijat ja liittää heihin työrooli, jonka perusteella käyttövaltuudet voidaan myöntää.	
Väliaikaisten oikeuksien hallinta	Henkilöiden tai toimijoiden rekisteröinti ennen työsuhteen alkua • Rekrytointijärjestelmään • Erilliseen väliaikaisten oikeuksien hallintajärjestelmään Esimies tekee alustavan työsopimuksen. Alustavan työsopimuksen tai työsuhteen pohjalta määritellään tarvittavat vähimmäistunnistetiedot oikeuksien luomista tai tilausprosessin käynnistämistä varten. Tämä on tilapäinen "temp - rekisteri". Sille asetetaan päättymispäivä (expiration time), jonka kuluessa on kohtuudella odotettavissa, että normaali tilausprosessi saadaan käyntiin ja työsopimus voimaan. Alustava työsopimus ja oikeudet tai tilausprosessi voidaan passivoida, jos rekrytointi epäonnistuu. Alustavan työsopimuksen pohjalta tehdään varsinainen työsopimus, jolloin tiedot siirtyvät rekrytointijärjestelmästä henkilöstöhallinnon järjestelmään.	Alustava työsopimus
Henkilötietojen hallinta	Henkilön perustietojen kirjaaminen ja ylläpito.	työntekijän perustiedot
Organisaatiotietojen hallinta	Organisaatiotietojen ylläpito	
Palvelusuhdetietojen hallinta	Toimijan palvelusuhteeseen liittyvien tietojen hallinta • Palvelusuhteen alku- ja päättymisajat, työsopimus • Henkilön sijoittuminen organisaatioon, yms.	palvelussuhdetiedot
Henkilön liittäminen työrooliin	Henkilö liitetään työrooleihin henkilön perustietojen rekisteröinnin yhteydessä. Rekrytoinnin yhteydessä on haettavat työroolit; työroolinimikkeet kiinnitetty. Käyttövaltuushallinnan puolella tapahtunut muutos henkilön työroolista otetaan vastaan ja päivitetään tarvittaessa henkilön tietoihin.	työntekijän työroolit

8.4 Hallinnointiprosessit



Kuva 8: Hallinnointiprosessi – eri prosessien välinen tietovirta

Edeltävät tehtävät ovat sellaisia, jotka tulee olla määriteltynä ja tehtynä ennen käyttövaltuushallinnan muiden prosessien kuvaamista. Edeltävien tehtävien prosessikuvauksia ei kuvata tässä dokumentaatiossa, koska ne on kuvattu muissa sidosarkkitehtuureissa ja ohjeissa (mm. VAHTI-ohjeet). Yleisesti kuitenkin mainittakoon, mitä tarkoitetaan käyttövaltuuksien hallintapolitiikalla:

- Organisaatiolla tulee olla olemassa käyttövaltuuksien hallintapolitiikka, jossa määritellään organisaation käyttövaltuusperiaatteet ja toimintatavat (VAHTI)
- Käyttövaltuuksien hallintapolitiikka johdetaan riskianalyysin pohjalta ja se on osa tietoturvapolitiikkaa.
- Hallintapolitiikan ja periaatteiden määrittelyssä on otettava huomioon organisaation nykyinen tila ja kyvykkyys. Nämä vaikuttavat siihen miten käyttövaltuushallinnassa edetään.
- Hallintapolitiikassa määritellään yleiset käyttäjien kirjautumisen ja tunnistamien periaatteet sekä käyttäjien käyttäjätunnusten ja salasanojen hallinnointiperiaatteet (Vahti-suositusten ja järjestelmäkäytäntöjen ja elinkaarten huomioiminen).

Tärkeä lähtökohta käyttövaltuushallinnan näkökulmasta on nykytilan järjestelmäsalkun kuvaaminen tai päivitys, järjestelmien elinkaarten määrittely sekä arviointi käyttövaltuushallinnan näkökulmasta. Jos näitä ei ole tehty, ovat ne etenemisen osalta yksi edeltäviä tai ensimmäisiä tehtäviä.

Käyttövaltuusrekisterin suunnittelu ja rekisteriselosteen laadinta

- Käyttövaltuusrekisteristä muodostuu henkilötietolain tarkoittama henkilörekisteri, josta tulee laatia rekisteriseloste. Rekisteriselostelomake löytyy tietosuojavaltuutetun toimiston sivuilta http://www.tietosuoja.fi/.

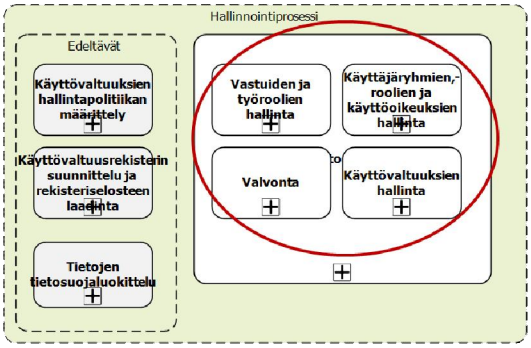
Tietojen tietosuojatasoluokittelu

- Suojattavat kohteet on tunnistettu ja tiedot on luokiteltu tietosuojauksen näkökulmasta.
- Tietoihin liittyvistä käyttövaltuuksista ja käyttövaltuuksien myöntämisestä päättää tietojen omistaja.
- Tietosuojaluokittelussa käytetään Julkisen hallinnon yleisiä tietosuojaluokittelutasoja (Vahti, JHS- ohjeet ja suositukset).

Kaikilla organisaation tiedoilla ja tietoja hallinnoivilla järjestelmillä on vastuullinen omistaja. Vastuiden määrittely tehdään organisaatiokohtaisesti.

Tietojen ja järjestelmien omistajan vastuulla on:

- Määritellä riskianalyysiin perustuva suojaamistarve.
- Päättää ja valvoa, ketkä tietoihin ja niitä hallinnoiviin tietojärjestelmiin pääsevät ja millä ehdoilla sekä millä käyttövaltuuksilla niihin päästään ja milloin oikeudet päättyvät. Oikeudet myönnetään työroolipohjaisesti.
- Määritellä vastuut siitä, kuka myöntää käyttöoikeudet eri järjestelmiin ja kuka niitä ylläpitää.
- Ylläpitää ajan tasalla olevaa luetteloa vastuullaan olevien tietojen käyttövaltuuksien haltijoista ja huolehtii käyttövaltuuksien auditoinneista.



Kuva 9: Kuvattavat hallintoprosessit ympyröitynä

Hallintoprosessin keskeisimmät prosessit ovat

- Vastuiden ja työroolien hallinta

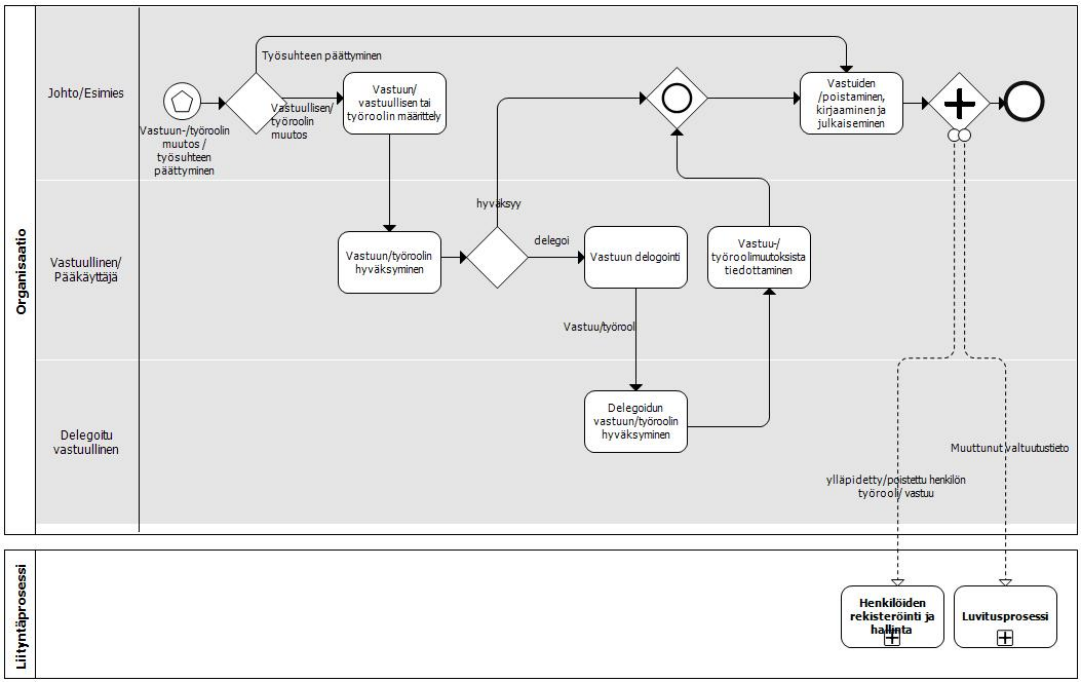
- Käyttäjäryhmien, -roolien ja käyttöoikeuksien hallinta
- Valvonta
- Käyttövaltuuksien hallinta

Prosessit ovat kuvattu tarkemmin alla olevissa kappaleissa.

Prosesseissa kuvatut yleiset roolit:

- Johto/esimies tarkoittaa päätösvaltaista johtavaa henkilöä tai työntekijän esimiestä kuntaorganisaatiossa. Johto/esimies kykenee vastuuttamaan tehtäviä alaisilleen.
- Johto/omistaja tarkoittaa päätösvaltaista henkilöä, joka on tietyn asian omistaja. Kaikissa kunnissa ei 'omistaja'-termiä ole käytetty, vaan asian hallinta ja siihen liittyvät päätökset kuuluvat johtavalle henkilölle.
- Vastuullinen/pääkäyttäjä tarkoittaa työntekijää, jolle on vastuutettu toimintoja, jotka tukevat käyttövaltuushallinnan toimintaa. Vastuullinen on usein kuvattu kuntaorganisaatiossa 'pääkäyttäjä'- tai 'vastuullinen pääkäyttäjä' -termillä.
- Käyttäjä/toimija kuvaa valtuutettua henkilöä, työtekijää tai asiakasta / asiakkaan puolesta toimijaa, ulkopuolista organisaatiota tai sen työntekijää, asiayhteydestä riippuen.

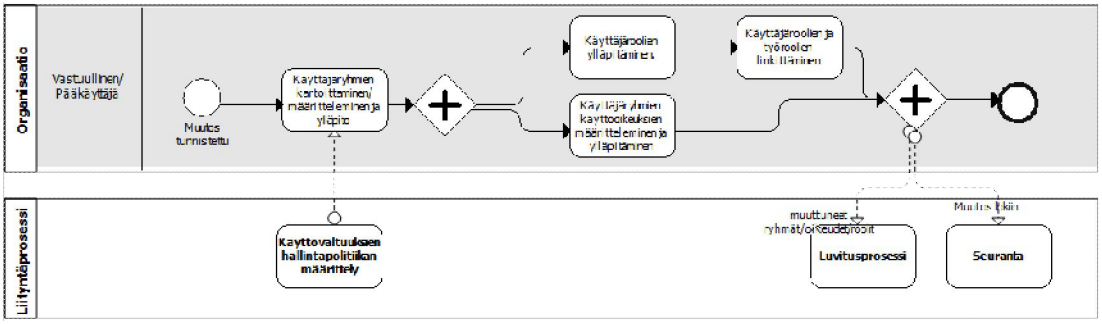
8.4.1 Vastuiden ja työroolien hallinta



Prosessi /tehtävä	Kuvaus	Tiedot/tulos

Vastuun, vastuullisen tai työroolin määrittely	Johto/esimies nimeää vastuulliset ja määrittelee vastuut tai kiinnittää työroolit	vastuut määritelty
Vastuun tai työroolin hyväksyminen	Vastuullinen hyväksyy hänelle osoitetun vastuun tai työroolin	Vastuut nimetty
Vastuiden delegointi	Vastuullinen tai vastuullinen pääkäyttäjä voi delegoida vastuut tai työroolin toiselle henkilölle. Esim. sovelluksen omistaja voi delegoida järjestelmän tai palvelun käyttäjäryhmien ja oikeuksien hallinnan sovellusten pääkäyttäjälle. Tai vastuullinen voi delegoida työroolinsa mukaiset tehtävät tai osan tehtävistä toiselle henkilölle esimies-alainen suhteessa. Vastuullinen voi delegoida vastuun vastuukautensa aikana.	vastuut delegoitu tai tarkennettu
Delegoidun vastuun tai työroolin hyväksyminen	Delegoitu vastuullinen eli vastuullinen, jolle on delegoitu vastuita, hyväksyy hänelle delegoidut vastuut tai työroolit.	hyväksytyt delegoidut vastuut
Vastuu- tai työroolimuutoksista tiedottaminen	Vastuullinen tiedottaa delegoimistaan vastuista tai työrooleista.	
Vastuiden poistaminen, kirjaaminen ja julkaiseminen	Johto/esimies ilmoittaa, kirjaa ja julkaisee tiedon vastuiden tai työroolien muutoksista tai työsuhteen päättymisestä aiheutuvien vastuiden tai työroolien poistamisesta. Johto/esimies ilmoittaa henkilöstöhallintoon työroolien tai vastuiden muuttumisesta. Muutostiedot tallentuvat luvitusjärjestelmään, josta ne prosessoidaan toteutukseen.	

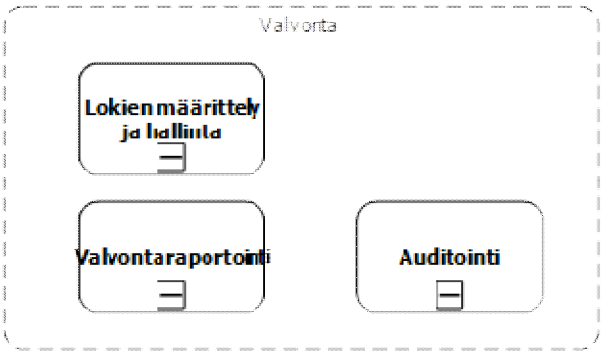
8.4.2 Käyttäjäryhmien, -roolien ja käyttöoikeuksien hallinta



Prosessi /tehtävä	Kuvaus	Tiedot/tulos
Käyttäjäryhmien	Vastuullinen/vastuullinen pääkäyttäjä kartoittaa	

kartoittaminen tai määritteleminen ja ylläpito	ja määrittelee tarvittavat käyttäjäryhmät. Käyttäjäryhmät määritellään järjestelmän toiminnoittain tai asiaperusteisesti loogisiksi kokonaisuuksiksi. Määrittelyssä kiinnitetään huomio erilaisten käyttäjien käyttötarpeeseen. Käyttäjäryhmät ja luettelot ylläpidetään muutosten mukaisesti.	
Käyttäjäroolien ylläpitäminen	Vastuullinen/vastuullinen pääkäyttäjä määrittelee ja ylläpitää käyttäjäryhmäkohtaiset käyttäjäroolit. Käyttäjäroolit saavat oikeudet käyttäjäryhmän mukaisesti.	ylläpidetyt käyttäjäroolit
Käyttäjäryhmien käyttöoikeuksien määritteleminen ja ylläpitäminen	Vastuullinen/vastuullinen pääkäyttäjä määrittelee oikeudet järjestelmään tai palveluun käyttäjäryhmittäin. Käyttäjäryhmä voi olla asiaperusteisesti muodostettu, jolloin oikeudet kirjataan vain ko. kokonaisuuteen.	käyttäjäryhmien oikeudet määritelty
Käyttäjäroolien ja työroolien linkittämine	Vastuullinen/vastuullinen pääkäyttäjä linkittää muuttuneet käyttäjäroolit työrooleihin. Työroolille voidaan myöntää useampi käyttäjärooli tarpeen mukaan. Tietoja ylläpidetään matriisissa.	työrooli-käyttäjärooli -matriisi päivitetty
Liittymäprosessit		
Käyttövaltuuksien hallintapolitiikan määrittely	Käyttövaltuuksien hallintapolitiikan määrittelyprosessin lopputuloksena tuotettu politiikka ohjaa käyttäjätunnusten ja käyttäjäryhmien määrittelyä.	
Seuranta	Muutoksista kirjataan muutoslokitieto.	muutoslokitieto
Luvitusprosessi	Luvitusprosessi hallitsee päivitykset kaikkiin kohdejärjestelmiin ja hakemistoon.	muuttuneet käyttäjäroolit päivitetty

8.4.3 Valvonta

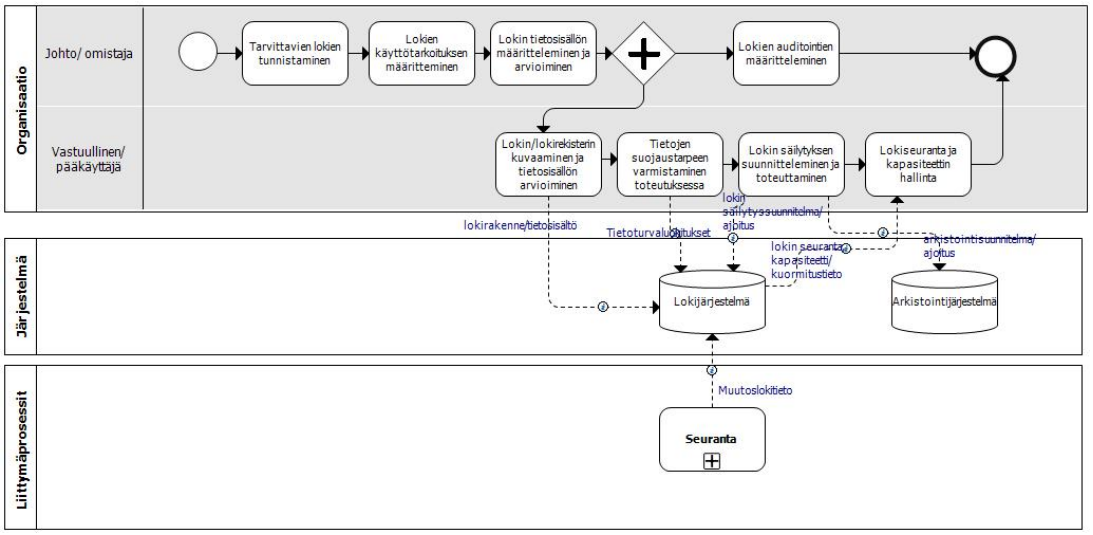


Kuva 10: Valvonnan osakokonaisuudet

Valvonta koostuu osakokonaisuuksista:

- Lokien määrittely ja hallinta, josta on erillinen prosessikuvaus alla.
- Valvontaraportointi, jossa tulee tarkastella ja määritellä seuraavat valvottavat asiat:
  - Käyttöoikeuksien ja valtuuksien valvonta: Onko käytössä turhia käyttöoikeuksia tai valtuuksia ja ovatko käyttöoikeudet ja valtuudet ajantasaisia.
  - Mitä on muuttunut (valtuudet, suojaustarpeet), koska muutos on tapahtunut, kenen toimesta muutos on tehty.
  - Onko jollekin myönnetty valtuuksia, joita ei pitäisi olla, esimerkiksi vaarallisia yhdistelmiä, jne.
  - Historiointi, jotta pystytään tarkastamaan kenellä on ollut valtuudet tiettynä ajankohtana. Näin varmistetaan jäljitettävyys.
  - Valvontaraportteja tulisi saada myös niistä järjestelmistä, jotka toimivat hakemistosta erillisinä. Tämä on mahdollista esimerkiksi seuraavin tavoin:
    - Manuaalisesti pääkäyttäjille lähetettävien pyyntöjen avulla.
    - Automaattisesti. Automaattiratkaisussa arvioitava, kannattaako sellaista tehdä, esim. mikä on kohteena olevien järjestelmien elinkaari.
- Auditointiprosessia kuvattaessa tulee kiinnittää huomio seuraaviin lähtökohtiin:
  - Auditointia ei suoriteta automaattisesti
  - Auditointi kohdistuu lokikantaan; suojaukseen ja sen toimivuuteen
  - Auditointien yhteydessä tulee varmistaa, että lokien kerääminen on teknisesti riittävällä ja luotettavalla tavalla toteutettu ja lokeihin liittyvät vaatimukset on tunnistettu.

Lokien määrittely ja hallinta –prosessikuvaus



Prosessi /tehtävä	Kuvaus	Tiedot/tulos
Tarvittavien lokien määrittelemi-nen	Johto (tietohallintojohto), tietojen omistaja tai vastuullinen tunnistavat tarvittavat lokit noudattaen yleisiä suosituksia ja ottamalla huomioon	tarvittavat lokit määritelty

	lainsäädännön vaatimukset.	
Lokien käyttötarkoitusten määritteleminen	Johto/omistaja määrittele mihin tarkoitukseen lokia tarvitaan ja miksi sitä tarvitaan, kuka käsittelee lokia ja millä oikeuksin.	
Lokin tietosisällön määritteleminen ja arvioiminen	Johto/omistaja määrittelee, mitä tietoa lokiin tallennetaan, arvioi tietojen tarpeellisuuden sekä tiedon keräämisen määrän kasvun ja käyttötiheyden.	
Lokien auditointien määritteleminen	Johto/omistaja määrittelee miten ja minkälaisin aikavälein lokikantaa auditoidaan sekä ketkä ovat valtuutettuja auditoimaan lokikannan sisältöä. Johto/omistaja määrittelee, onko tarpeen auditoida lokimenettelyä yleensä.	auditointisuunnitelma
Lokin ja lokirekisterin kuvaaminen ja tietosisällön arviointi	Vastuullinen/vastuullinen pääkäyttäjä kuvaa tarvittavan lokin rekisteriselosteen, sen sisältämät tiedot ja lokin rakenteen yleisesti käytettyjen lokimallien mukaan sekä arvioi tietosisällön koon pidemmällä aikavälillä.	lokit kuvattu
Tietojen suojaustarpeen varmistaminen toteutuksessa	Vastuullinen/vastuullinen pääkäyttäjä arvioi lokin sisältämien tietojen suojaamistarpeen tietojen tietoturvaluokituksen perusteella ja varmistaa, että lokin käyttövaltuudet on määritelty suojaustarpeita vastaaviksi. Vastuullisen tulee varmistaa lokien käyttö ja tarkoituksenmukainen hallinta.	Turvallinen lokiympäristö suunniteltu ja luotu
Lokin säilytyksen suunnitteleminen ja toteuttaminen	Vastuullinen/vastuullinen pääkäyttäjä suunnittelee lokin säilytyksen ja säilytyksen totutukseen tarvittavan arkistoinnin lainsäädännön ja muiden ohjeiden mukaisesti. Vastuullinen suunnittelee, miten tiedot tarvittaessa siirretään aktiivisesta lokikannasta arkistointikantaan määriteltyjen aikavälien mukaisesti. Huomioi Lokitietojen säilytysajoissa arkistolaki (831/94)	Lokien arkistointi suunniteltu ja luotu
Lokiseuranta ja kapasiteetin hallinta	Vastuullinen/vastuullinen pääkäyttäjä seuraa lokikannan tilannetta, kirjaamistapahtumien lukumäärää, kuormitusta, kapasiteettitarvetta	kuormitus/ kapasiteettiraportti
Liittymäprosessit		
Seuranta	Kirjaa muutostapahtumista lokitiedon muutoslokiin	

8.4.4 Käyttövaltuuksien hallinta

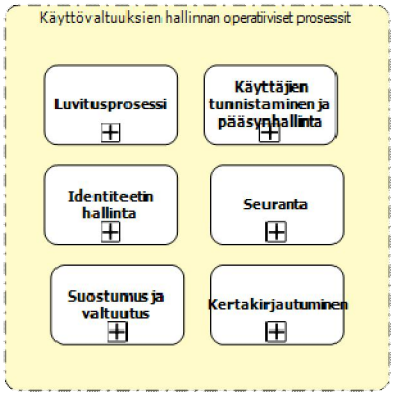
Käyttövaltuudet määritellään ja ylläpidetään käyttövaltuuksien hallintapolitiikan mukaisesti. Käyttövaltuuksien hallinnasta ei ole erillistä prosessikuvausta.

Käyttövaltuuksien hallintaan liittyy seuraavia määrittelytehtäviä:

- Määritellään ja ylläpidetään työroolin mukaiset valtuudet
- Linkitetään työroolit kohdejärjestelmien käyttäjäryhmiin (Liite 3: työrooli ja käyttäjärooli matriisi)
- Määritellään muut tarvittavat valtuudet:
  - Käyttövaltuudet sisältävät myös ”fyysisiä valtuuksia” (viite: VIRTUK)
    - Sirullinen nimikortti, henkilökortti
    - Vierailijakortti
    - Kulkuluvat, kulkuoikeudet fyysisiin tiloihin
    - Parkkioikeudet ja pysäköintiluvat
    - Avaimet

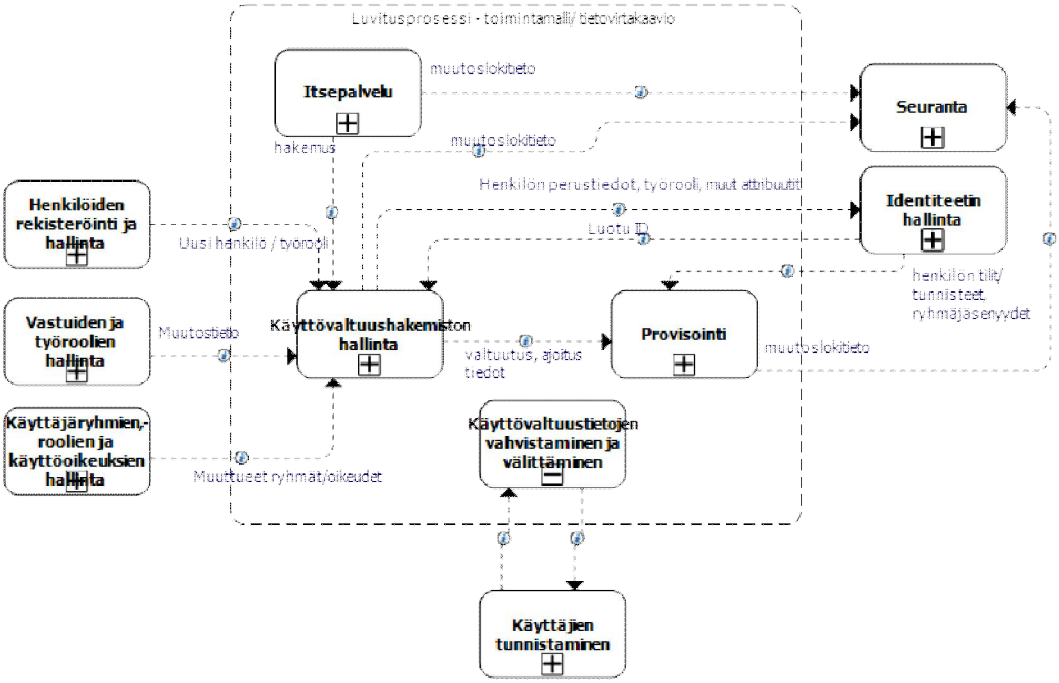
8.5 Operatiiviset prosessit

Operatiivisissa prosesseissa kuvataan keskeisimmät prosessit jotka tulee toteuttaa käyttövaltuushallinnan onnistumiseksi sekä niiden väliset suhteet. Operatiiviset prosessit on jaoteltu osakokonaisuuksiin, joiden voidaan ajatella toimivan itsenäisinä kokonaisuuksina.



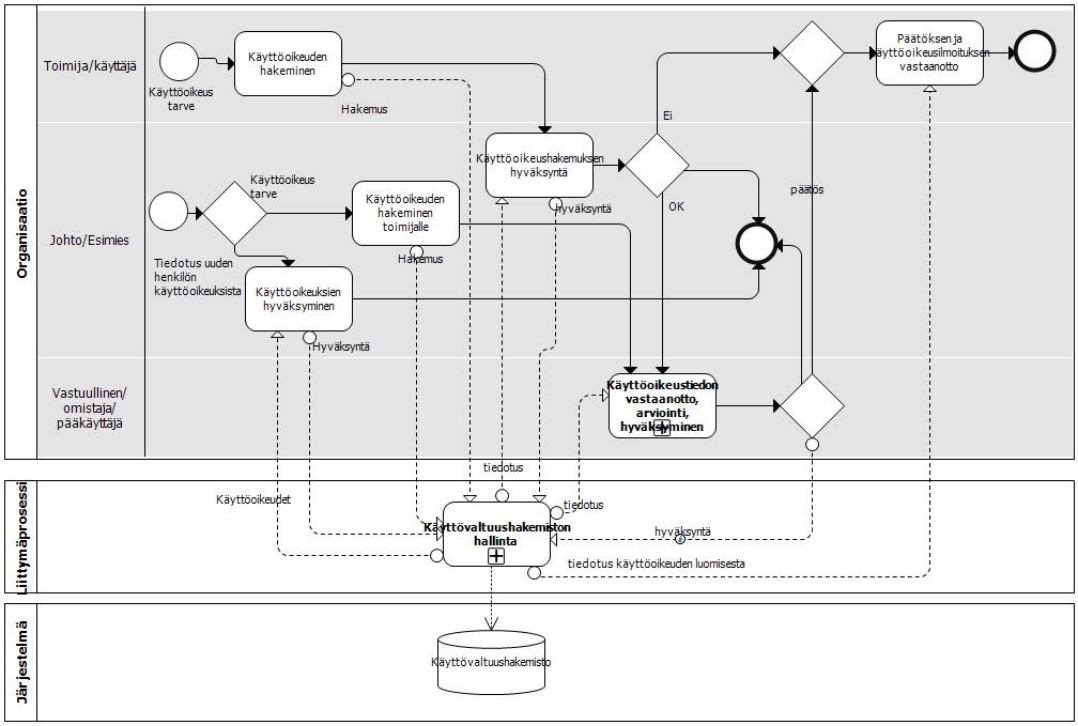
8.5.1 Luvitusprosessi

Luvitusprosessi sisältää kaikki käyttövaltuuksien hallintaan ja jakeluun liittyvät tehtävät kuten lisävaltuuksien hakemiset itsepalveluperiaatteella, käyttövaltuushakemiston päivitykset, valtuuksien provisioinnit kohdejärjestelmiin (myös manuaalinen käsittely) sekä myös valtuutuskyselyjen käsittelyn. Alla olevassa kuvassa on kuvattuna luvitusprosessin integraatio ja tietovirrat sen liittymäprosesseihin. Luvitusprosessin osat on kuvattu tarkemmin alla olevissa kappaleissa.



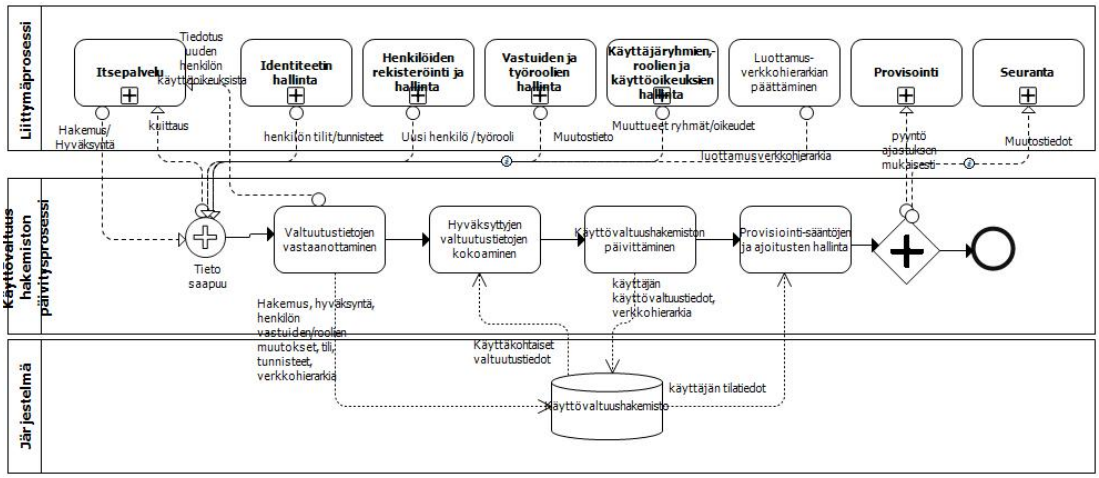
Kuva 11: Luvitusprosessin toimintamalli ja tietovirrat

Itsepalvelu- osaprosessi



Prosessi /tehtävä	Kuvaus	Tiedot/tulos
A) Käyttöoikeuden hakeminen B) Käyttöoikeuden hakeminen toimijalle	A) Käyttäjä hakee lisäkäyttövaltuuksia ja käyttöoikeuksia itsepalveluportaalin kautta B) Käyttäjän esimies hakee lisäkäyttövaltuuksia ja käyttöoikeuksia toimijalle itsepalveluportaalin kautta. (lisäkäyttövaltuudet pitää erikseen hakea. Niitä ei saada automaattisesti työroolien kautta))	Hakemus
Käyttövaltuushakemuksen hyväksyminen	Esimies hyväksyy käyttäjän tekemän hakemuksen	Hyväksytty hakemus
Käyttöoikeuksien hyväksyminen	Tarvittaessa esimies vastaanottaa tiedotuksen ja hyväksyy uuden työtekijän työroolin mukaiset käyttövaltuudet (lista).	Hyväksytyt valtuudet
Käyttöoikeustiedon vastaanotto, arviointi, hyväksyminen	A) Vastuullinen/pääkäyttäjä vastaanottaa tiedon hakemuksesta B) Vastuullinen/pääkäyttäjä vastaanottaa, arvioi (huomioiden kielletyt yhdistelmät) ja hyväksyy hakemuksen	
Päätöksen ja käyttöoikeusilmoituksen vastaanotto	Käyttäjä/toimija vastaanottaa päätöksen saamistaan lisäkäyttövaltuuksista.	Vastaanotettu tieto lisäkäyttövaltuuksista
Liittymäprosessi		
Käyttövaltuushakemiston hallinta	Luvitusjärjestelmä vastaanottaa pyynnön ja kirjaa pyynnön lokiin ja tiedottaa vastuullista tai esimiestä. Järjestelmä päivittää käyttövaltuushakemiston ja syöttää käyttöoikeudet automaattisesti ja reaaliaikaistesti tai ehtojen mukaisesti. Järjestelmä välittää luvituspyynnön pääkäyttäjälle, joka suorittaa luvituksen pyynnön mukaisesti ja kuittaa sen tai Luvituspyyntö ajastetaan kohdejärjestelmän työjonoon, josta luvitus astuu voimaan ehtojen mukaisesti. Järjestelmä tiedottaa käyttöoikeuksien luomisesta käyttäjää.	Viesti hakemuksesta Tiedotus käyttöoikeuksien luomisesta

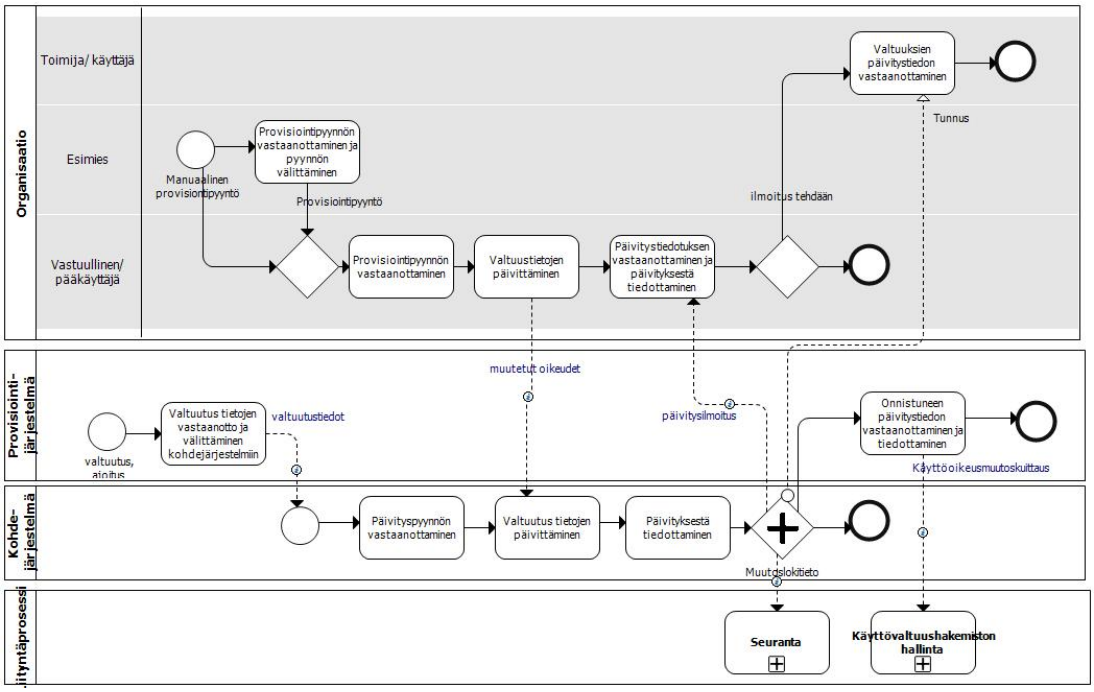
Käyttövaltuushakemiston hallinnan- osaprosessi



Prosessi /tehtävä	Kuvaus	Tiedot/tulos
Valtuutustietojen vastaanotto	Käyttövaltuushakemiston päivitysprosessi vastaanottaa saapuvat valtuutuspyynnöt ja tietojen täydennykset. Valtuutuspyyntöjä voi tulla useammasta eri prosessista: • Valtuutuspyyntö uuden henkilön rekisteröinnin myötä (ennakko, varsinainen) • Muutospyyntö työroolien ja vastuiden muuttuessa • Muutospyyntö käyttäjäryhmien, käyttäjäryhmien oikeuksien muuttuessa • Luottamusverkkohierarkian päivityspyyntö	Vastaanotetut tiedot ja valtuudet
Valtuutustietojen kokoaminen	Käyttövaltuushakemiston päivitysprosessi kokoaa toimijaan liittyvät ja saapuneet tiedot sekä valtuudet yhteen	Käyttäjäkohtaiset kootut tiedot ja valtuudet
Käyttövaltuushakemiston päivittäminen	Prosessin mukaan kootut, hyväksytyt toimijaan/käyttäjään liittyvät tiedot ja valtuudet tai luottamusverkkoon liittyvät kootut tiedot päivitetään hakemistoon.	Hakemistoon päivitetyt käyttäjäkohtaiset tiedot ja valtuudet
Provisiointisääntöjen ja ajoitusten hallinta	Käyttövaltuushakemiston päivitysprosessi päättelee ajoitukset sekä hallitsee sääntöjä, joiden perusteella provisiointi hoidetaan ja tahdistetaan. Prosessi tarkistaa mahdollisesti syntyneet kielletyt yhdistelmät käyttäjän työroolin tai vastuiden mukaisten valtuuksien muuttuessa. Prosessi tiedottaa umpeutuvista käyttövaltuuksista esimiehille.	tarkistetut käyttövaltuudet
Liittymäprosessit		
Seuranta	Käyttövaltuushakemiston päivityksen yhteydessä kirjataan toimenpide lokiin.	muutoslokitieto
Provisiointi	Provisiointiprosessille lähetetään ajoituksen ja	provisiointipyyntö

	ehtojen mukaisesti pyyntö.	

Provisiointi- osaprosessi



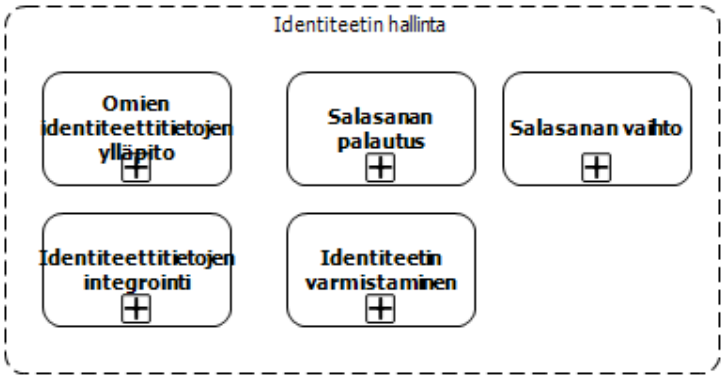
Prosessi /tehtävä	Kuvaus	Tiedot/tulos
Provisiointipyynnön vastaanottaminen ja pyynnön välittäminen	Esimies vastaanottaa manuaalisen provisiointipyynnön ja välittää sen vastuulliselle pääkäyttäjälle/vastuulliselle, joka toteuttaa pyynnön.	manuaalipyyntö vastaanotettu ja siirretty vastuutetulle
Pyynnön vastaanottaminen	Vastuullinen/vastuullinen pääkäyttäjä vastaanottaa manuaalisen provisiointipyynnön ja siirtää sen käsittelyyn.	pyyntö vastaanotettu
Päivitystiedotuksen vastaanottaminen ja päivityksestä tiedottaminen	Vastuullinen/vastuullinen pääkäyttäjä saa tiedon päivityksestä ja tiedottaa vastuiden päivityksestä toimijaa/käyttäjää.	
Valtuutustietojen vastaanotto ja välittäminen kohdejärjestelmiin	Provisiointijärjestelmä vastaanottaa valtuutuspyynnöt ja välittää ne pyynnön mukaisiin kohdejärjestelmiin tai palveluihin. Samassa yhteydessä päivittyy tarvittaessa salasanakukkaro, jos salasanoja on palautettu tai muutettu.	valtuutuudet siirretty kohdejärjestelmille
Päivityspyynnön vastaanottaminen	Kohdejärjestelmä vastaanottaa valtuutuspyynnön.	
Valtuutustietojen päivittäminen	Kohdejärjestelmä päivittää valtuutukset (fyysinen päivitys) tarvittaviin kohteisiin.	valtuudet päivitetty järjestelmään

Päivityksestä tiedottaminen	Kohdejärjestelmä tiedottaa (kuittaus) päivityksen onnistumisesta pääkäyttäjää/järjestelmä vastuullista tai provisiointijärjestelmää.	päivityksen kuittaus
Valtuuksien päivitystiedon vastaanottaminen	Tomija/käyttäjä vastaanottaa tiedon valtuuksista.	tunnukset /tiedotus vastaanotettu
Onnistuneen päivitystiedon vastaanottaminen ja tiedottaminen	Provisiointijärjestelmä tiedottaa hakemistolle käyttöoikeusmuutosten päivityksestä (hakemisto ylläpitää tilatietoa).	käyttöoikeusmuutoskuittaus
Liittymäprosessit		
Seuranta	Kohdejärjestelmä kirjaa lokiin päivityksen.	
Käyttövaltuushakemiston hallinta	Provisiointijärjestelmään ilmoitus valtuutuspäivityksestä.	

Käyttövaltuustietojen vahvistaminen ja välittäminen osaprosessi

Prosessissa liitetään henkilö oikeisiin käyttövaltuusryhmiin tiketin tietojen perusteella. Ulkoisen identiteetinhallinnan tunniste vaihdetaan organisaation sisäiseen työrooliin. Tarvittaessa työrooli tulee valita (käyttäjään liittyy useita työrooleja).

8.5.2 Identiteetin hallinta



Kuva 12: Identiteetin hallintaprosessin osakokonaisuudet

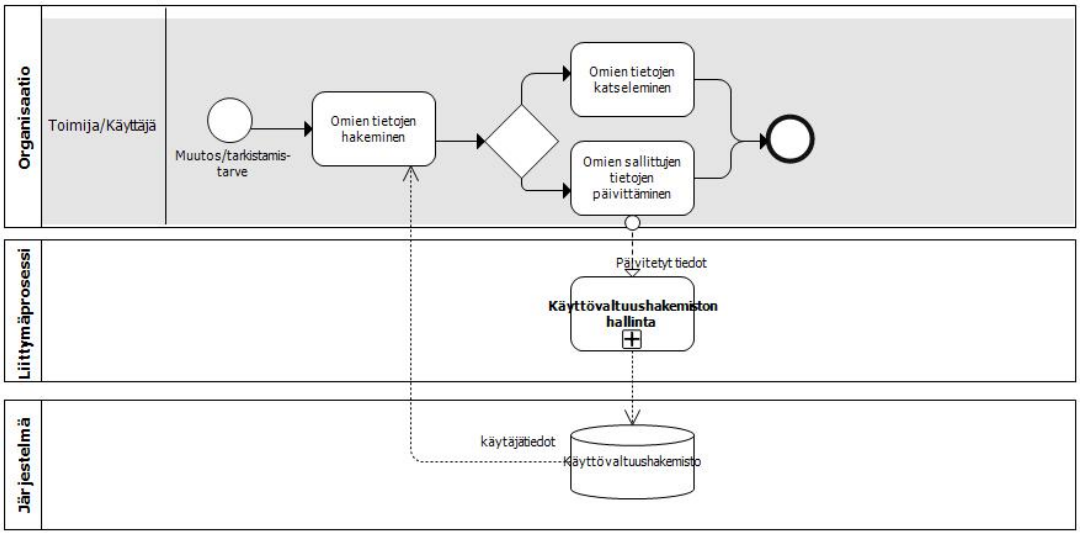
Identiteetin hallintaprosessissa käsitellään identiteetin ja siihen liittyvien tietojen hallintaa (luominen, ylläpito, integrointi). Identiteetin hallinta jakaantuu seuraaviin osakokonaisuuksiin:

- Omien identiteettitietojen ylläpito
  - Toimija voi katsella ja ylläpitää sallituin osin omia identiteettitietojaan.
- Identiteetin varmistaminen

- Käyttäjien identiteetti varmistetaan ja varmistetuille toimijoille tai käyttäjille luodaan yksilöllinen identiteettitunnus.

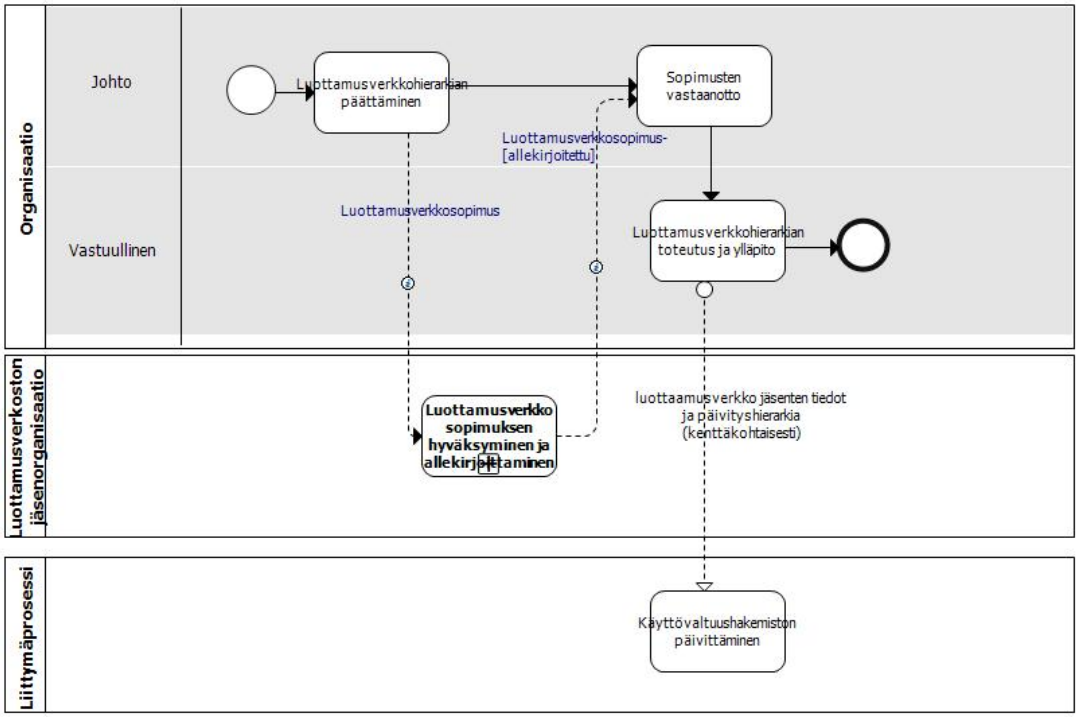
- Salasanan palautus
  - Toimija voi pyytää palauttamaan unohtuneen salasanan.
- Salasanan vaihto
  - Toimija voi vaihtaa salasanan kohdejärjestelmään.
- Identiteettitietojen integrointi (ulkoa tulevat tunnistetiedot)
  - Luottamusverkkoon perustuvat identiteettitietojen hierarkiasäännöt

Omien identiteettitietojen ylläpito



Prosessi /tehtävä	Kuvaus	Tiedot/tulos
Omien tietojen hakeminen	Käyttäjä hakee omat identiteetti tietonsa.	haetut käyttäjän tiedot
Omien identiteet-titietojen katse-leminen	Käyttäjä voi selailla ja tarkistaa omia identifiointi-tietojaan.	
Omien sallittujen identiteettitieto-jen päivittäminen	Käyttäjä voi päivittää joitakin sallittuja omia tie-tojaan esimerkiksi osoitetietojaan, mutta ei esi-merkiksi identifioivan tunnuksen tietoja.	päivitetyt käyttä-jän tiedot
Liittymäprosessit		
Käyttövaltuusha-kemiston hallinta	Käyttäjän päivitetyt tiedot viedään hakemistoon päivitettäväksi.	

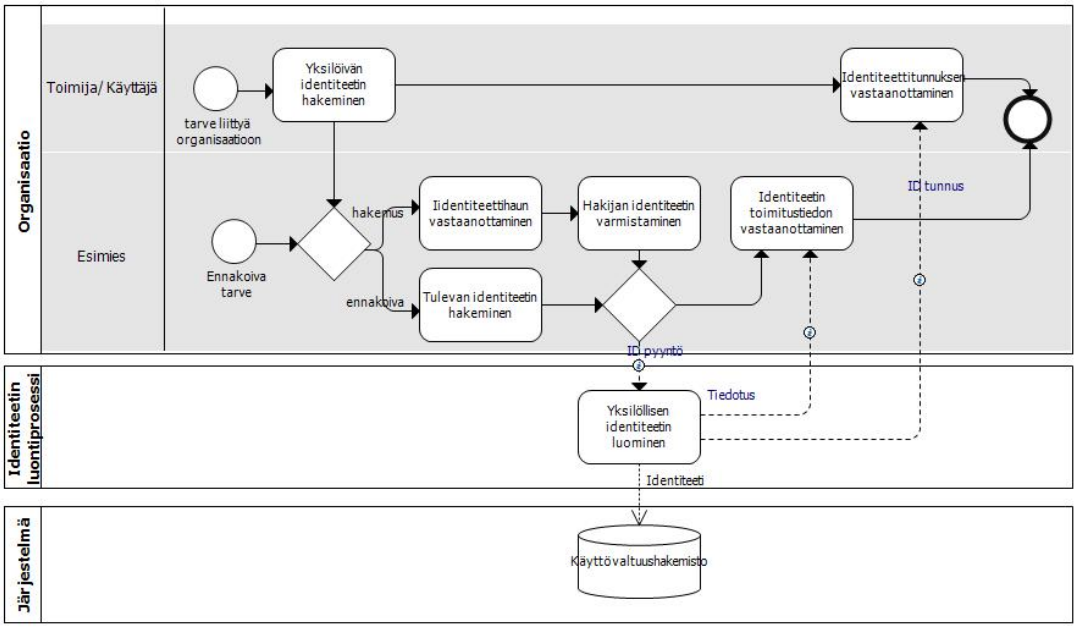
Identiteettitietojen integrointi



Prosessi /tehtävä	Kuvaus	Tiedot/tulos
Luottamusverkkohierarkian päättäminen	Johto päättää, keiden kanssa muodostetaan luottamusverkko ja minkä hierarkkisen järjestyksen mukaan eri hakemistoissa olevat eritasoiset tiedot päivitetään. Luottamusverkko muodostuu organisaatioista, kuntatoimijoista, jotka keskenään sopivat keskinäisestä yhteistyöstä määriteltyjen sääntöjen mukaisesti. Federaatiossa määritellään yleensä luottamuksen päähakemisto, luottamustahot ja attribuutit, sekä federointiin liittyvä metadata. Yleensä organisaatioilla on luottamusverkossa yksi pääsynhallinta (identity provider) -palvelu. Tunnistamiseen liittyen ja useita verkkopalveluita tai palveluita (Service Providers).	luottamusverkko, luottamusverkkohierarkia
Luottamusverkkosopimuksen hyväksyminen ja allekirjoittaminen	Luottamusverkkohierarkian mukainen jäsenenorganisaatio hyväksyy luottamusverkon säännöt ja ehdot ja allekirjoittaa sopimuksen. Luottamusverkoston jäsen voi toimia luottamusverkostossa kotiorganisaationa ja palveluntarjoajana.	hyväksytty ja allekirjoitettu sopimus
Sopimuksen vastaanottaminen	Johto vastaanottaa luottamusverkon jäsenten hyväksynnän ja allekirjoitetun sopimuksen.	sopimukset kirjattu saapuneiksi
Luottamusverkkohierarkian to-	Vastuullinen toteuttaa luottamusverkkohierarkian ehtojen mukaisen rakenteen ja ylläpitää raken-	ehdot ja hierarkiarakenne määri-

teutus ja ylläpito	netta ja ehtoja.	telty ja toteutettu
Liittymäprosessit		
Käyttövaltuushakemiston päivittäminen	Hierarkkinen päivityssääntö viedään käyttövaltuushakemiston tilatietoihin.	Hakemisto ajantasalla

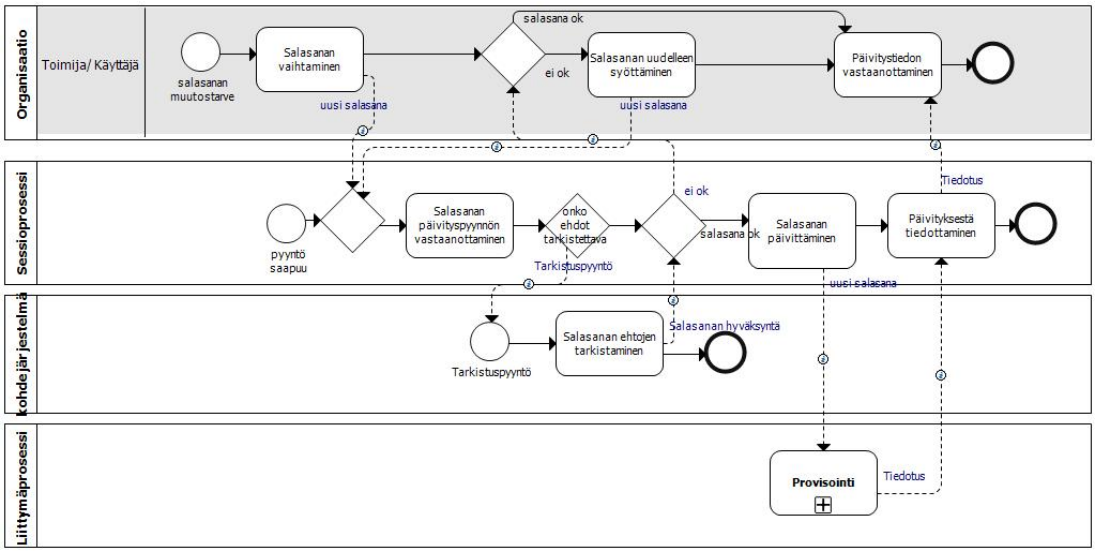
Identiteetin varmistaminen



Prosessi /tehtävä	Kuvaus	Tiedot/tulos
Yksilöivän identiteetin hakeminen	Toimijalla on tarve hakea identiteettitunnusta kohdeorganisaatioon.	identiteettihakemus
Identiteettihakemuksen vastaanottaminen	Vastuullinen esimies vastaanottaa identiteettihakemuksen.	vastaanotettu hakemus
Hakijan identiteetin varmistaminen	Vastuullinen esimies varmistaa hakijan identiteetin ja pyytää järjestelmää luomaan identiteettitunnuksen.	identiteetti varmistettu ja identiteettitunnukset pyydetty
Tulevan identiteetin hakeminen	Vastuullinen esimies voi ennakoivasti hakea toimijalle yksilöllistä, määräaikaista identiteettiä vajain varmistuksin.	ennakoitu identiteettitunnus pyydetty
Yksilöllisen identiteetin luominen	Järjestelmä luo yksilöllisen tunnuksen toimijalle ja tiedottaa tunnuksen luomisesta.	identiteetti luotu
Identiteetin toimitustiedon vastaanottaminen	Vastuullinen esimies vastaanottaa ilmoituksen tunnuksen onnistuneesta luomisesta.	tiedotus

Identiteettitunnuksen vastaanottaminen	Hakija vastaanottaa identiteettitunnuksen.	vastaanotettu ID-tunnus

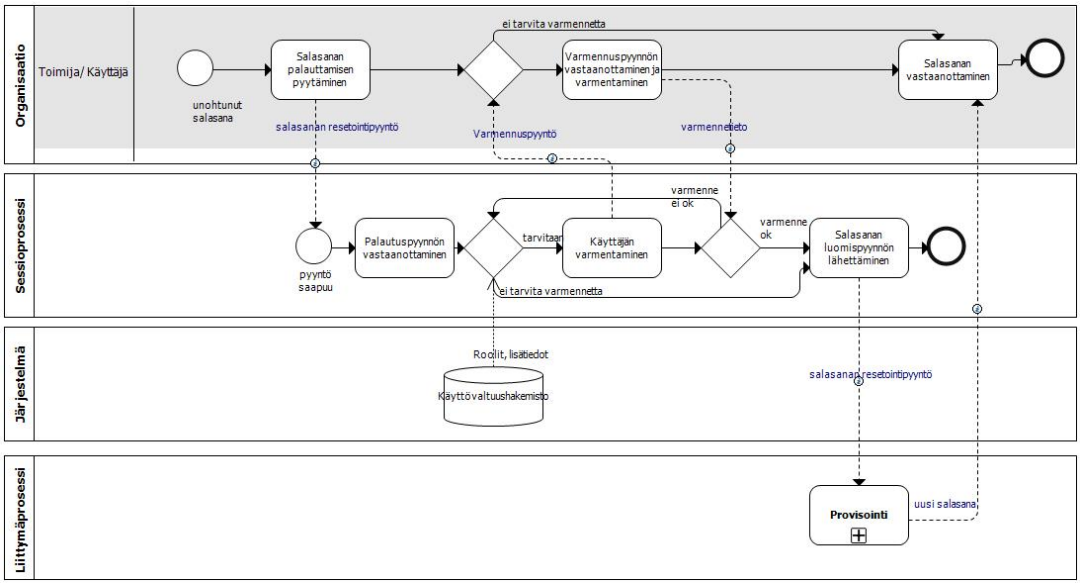
Salasanan vaihto



Prosessi /tehtävä	Kuvaus	Tiedot/tulos
Salasanan vaihtaminen	Toimija haluaa vaihtaa salasanan.	päivityspyyntö
Salasanan päivityspyynnön vastaanottaminen	Sessionhallintaprosessi vastaanottaa päivityspyynnön. Jo salasana on kertakirjautumisen hakemiston salasanan vaihtopyyntö, ei kohdejärjestelmästä tarvitse tarkistaa salasanaehtoja., muuten prosessi tarkistaa kohdejärjestelmästä, ovatko salasanan ehdot täyttyneet.	tarkistuspyyn
Salasanan ehtojen tarkistaminen	Kohdejärjestelmä tekee salasanan muodollisuustarkistuksen.	tarkistetut salasanan ehdot
Salasanan uudelleen syöttäminen	Toimija/käyttäjä syöttää tarvittaessa uuden salasanan uudelleen.	uusi salasana
Salasanan päivittäminen	Annettu salasana täytti ehdot ja hyväksyttiin uudeksi salasanaksi. Salasana päivitetään kohdejärjestelmiin provisiointiprosessin kautta.	hyväksytty uusi salasana
Päivityksestä tiedottaminen	Sessionhallintaprosessi tiedottaa toimijaa onnistuneesta päivityksestä.	
Päivittämistiedotuksen vastaanottaminen	Toimija vastaanottaa ilmoituksen onnistuneesta päivityksestä.	vastaanotettu päivitysilmoitus
Liittymäprosessit		

Provisiointi	Salasanan päivityspyyntö välitetään kohdejärjestelmään ja tarvittaessa salasanakukkaroon provisioinnin kautta.	uusi salasana provisioitu

Salasanan palautus

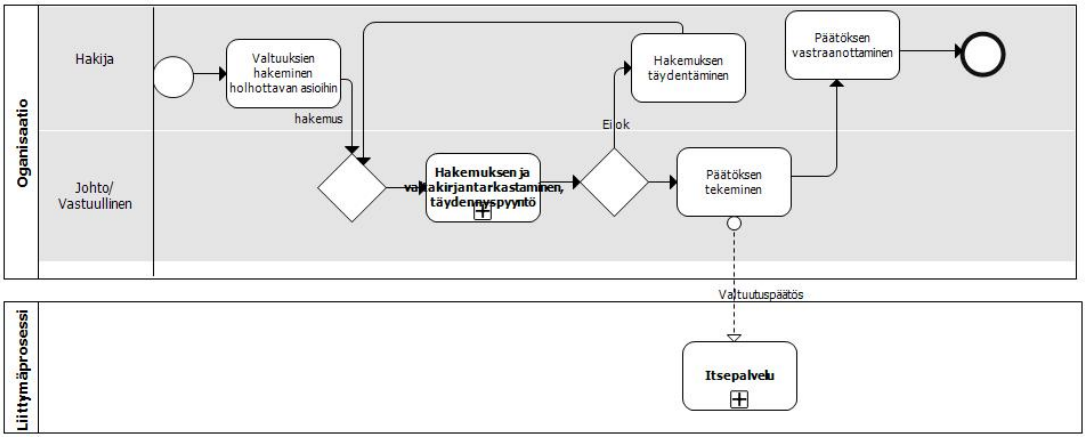


Prosessi /tehtävä	Kuvaus	Tiedot/tulos
Salasanan palauttamisen pyytäminen	Toimija pyytää salasanan palauttamista.	palautuspyyntö tehty
Palautuspyynnön vastaanottaminen	Sessioprosessi vastaanottaa pyynnön.	vastaanotettu pyyntö
Käyttäjän varmentaminen	Sessioprosessi hakee käyttövaltuushakemistosta toimijan roolitiedot ja lisätiedot varmentamisen pohjaksi.	varmennustiedot haettu ja varmennusta pyydetty
Varmennuspyynnön vastaanottaminen ja varmentaminen	Toimija vastaanottaa varmennuspyynnön ja varmentaa identiteettinsä.	
Salasanan luomispyynnön lähettäminen	Sessioprosessi lähettää salasanan palauttamispyynnön provisiointiprosessin kautta hakemistolle (kertakirjautumisen/ hakemiston salasanan päivitys) tai kohdejärjestelmälle.	
Salasanan vastaanottaminen	Toimija vastaanottaa luodun salasanan.	uusi salasana
Liittymäprosessit		
Provisiointi	Salasanan palauttamispyyntö välitetään kohdejärjestelmään ja tarvittaessa salasanakukkaroon	uusi salasana provisioitu

	provisioinnin kautta.	

8.5.3 Suostumus ja valtuutus

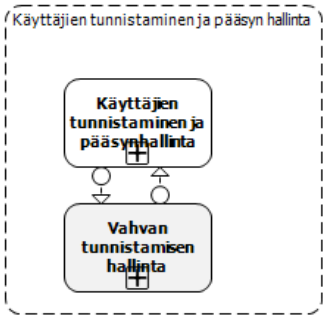
Jokaisesta toimenpiteestä, jossa valtuutettu hoitaa esim. valtakirjan perusteella toisen tahon asioita, pitää jäädä tiedot kuka hoiti, kenen asioita hoiti sekä mihin tämä valtuutus perustui. Tiedot pitää pystyä helposti hakemaan jälkikäteen katseltaviksi.



Prosessi /tehtävä	Kuvaus	Tiedot/tulos
Valtuutuksen hakeminen holhottavan asioihin	Hakija hakee valtakirjan perusteella valtuutuksia holhottavan asioihin.	hakemus
Hakemuksen ja valtakirjan tarkastaminen	Johto/vastuullinen vastaanottaa tiedon hakemuksen saapumisesta ja tarkastaa hakemuksen sekä valtakirjan ja pyytää tarvittaessa täydentämään hakemusta.	tarkistettu hakemus/valtakirja
Hakemuksen täydentäminen	Hakija täydentää hakemusta.	
Päätöksen tekeminen	Johto/vastuullinen päättäjä tekee hakemuksen ja valtakirjan pohjalta päätöksen myönnettävistä valtuuksista tai valtuuksien eväämisestä.	päätös
Päätöksen vastaanottaminen	Hakija vastaanottaa päätöksen.	päätös vastaanotettu
Liittymäprosessit		
Itsepalvelu	Hakijan valtuudet toteutetaan itsepalveluprosessin kautta.	

8.5.4 Käyttäjien tunnistaminen ja pääsynhallinta

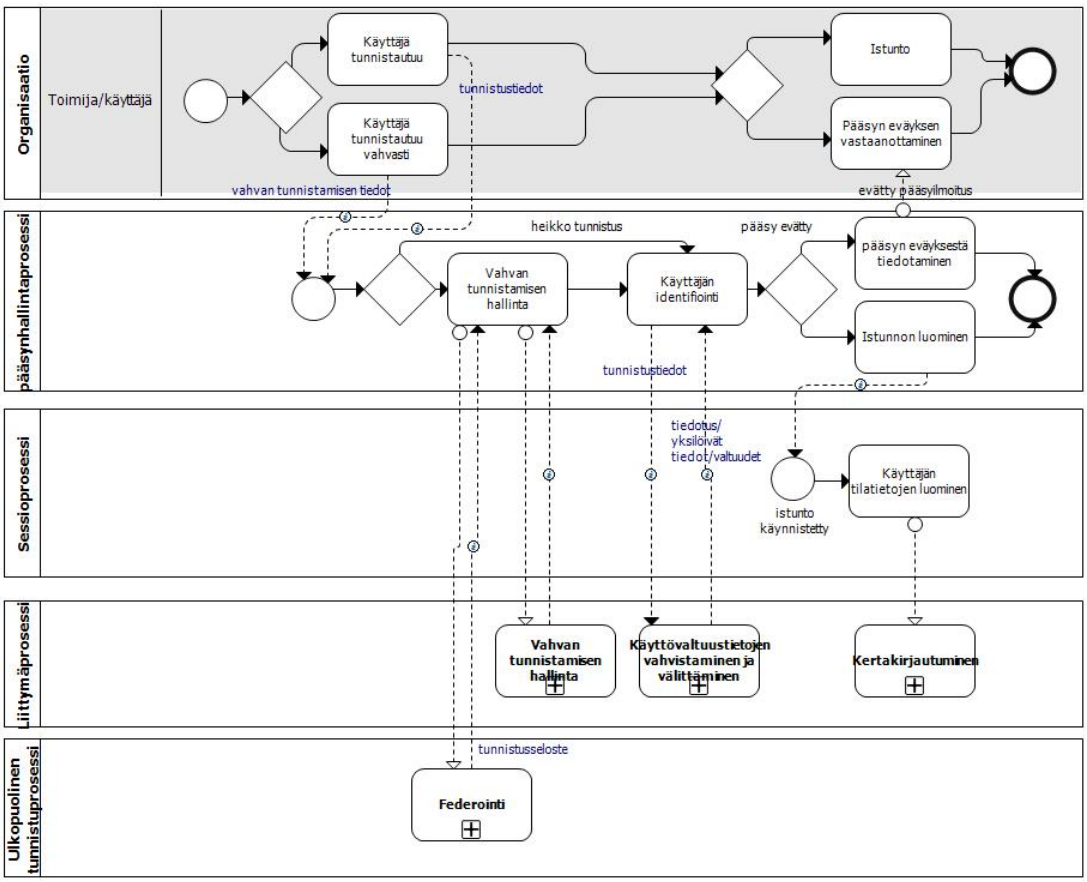
Tässä dokumentissa on kuvattu roolipohjainen pääsynvalvonta eli käyttäjärooleihin ja niihin liitettyihin käyttövaltuuksiin perustuva pääsynvalvonta. Pääsynhallintaprosessi on jaettu kahteen osaprosessiin (katso kuva alla).



Kuva 13: käyttäjien tunnistaminen ja pääsynhallinta osaprosessit

Vahvaan tunnistamisen hallintaprosessia ei kuvata tässä yhteydessä, koska tässä kuvauksessa ei oteta kantaa kyseisten menetelmien mallintamiseen/ tekniseen toteuttamiseen.

Käyttäjien tunnistaminen ja pääsynhallinta



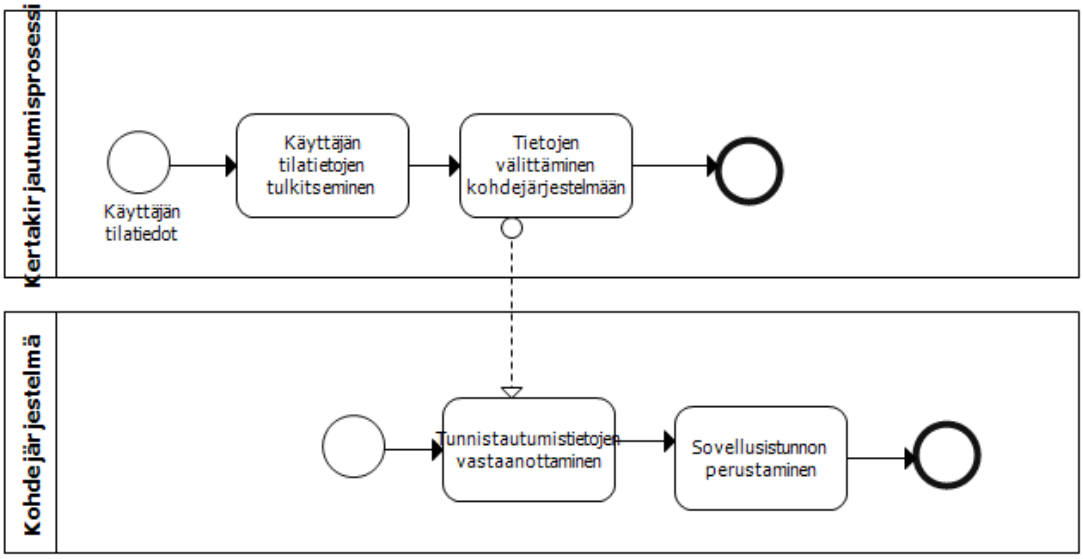
Prosessi /tehtävä	Kuvaus	Tiedot/tulos
Käyttäjä tunnistautuu	Käyttäjä tunnistautuu heikosti, käyttämällä käyttäjätunnusta ja salasanaa. Käyttäjä valitsee tarvittaessa kertakirjautumisen tunnistautumisen yhteydessä työroolin, jossa kirjautuu. Valitun työroolin perusteella kohdesovellukset ovat käytettävissä.	tunnistautuminen suoritettu
Käyttäjä tunnistautuu vahvasti	Käyttäjä tunnistautuu vahvasti käyttämällä jotain vahvan tunnistautumisen välinettä: • ulkoista (Vetuma/Tupas, Katso,…) • kunnan sisäistä (kuntakortti /terveydenhuollon kortti Käyttäjä valitsee tarvittaessa kertakirjautumisen tunnistautumisen yhteydessä työroolin, jossa kirjautuu. Valitun työroolin perusteella kohdesovellukset ovat käytettävissä..	vahva tunnistautuminen suoritettu
Vahvan tunnistamisen hallinta	Pääsynhallintaprosessi ohjaa ja ylläpitää tietoa tunnistamisesta ja tunnistamiseen liittyvistä tiedoista. Prosessi ohjaa sekä kunnan sisäistä vahvaa tunnistamista että federaation kautta tulevaa vahvaa tunnistamista (Virtu, Vetuma,..). Federaation kautta luotettavan tunnistuslähteen kautta tulevaan tunnistukseen luotetaan.	ulkopuolinen vahva tunnistus hyväksytty tunnistuksen takistuspyyntö lähetetty
Käyttäjän identifiointi	Pääsynhallintaprosessi identifioi käyttäjän tunnisteen perusteella, pyytämällä käyttövaltuushallinnan prosessilta tietoja. Pääsynhallinta vertailee saatuja yksilöintitietoja tai tunnistustietoja luottamusverkkohierarkiaa vasten, jonka perusteella pääsy voidaan sallia tai evätä. Pääsy voidaan evätä pääsy esim. seuraavissa tapauksissa: • Ulkoiselta tunnisteelta saadun käyttäjän tiedot eroavat hakemistossa olevista provisioiduista tiedoista tai valtuuksista • Pääsynhallinta päättelee mahdollisesti löydettyjen tietojen epäajantasaisuuden perusteella, mikä on luotettavaa tietoa • Käyttäjän tietoja ei löydy käyttövaltuushakemistosta (sisäinen tunnistautumistapa) • Tiedot eivät ole luotettavia, jolloin pääsy evätään	vahvistus tai pääsyn eväys
Käyttövaltuustietojen vahvistaminen ja välittäminen	Käyttövaltuushallinta tarkastaa tunnistautumistietojen mukaisen käyttäjän, luottamusverkkohierarkian, varmistaa valtuudet ja palauttaa tiedot, jos käyttäjä ja valtuudet olivat aktiivisia. Käyttövaltuushallinta muuntaa tarvittaessa ulkoisesta lähteestä saapuneen tunnistustiedot (”tiketin”) organisaation tunnistusselosteen mukaiseksi ja muodostaa käyttäjän istunnon aikaiset yksilöivät tiedot. Käyttövaltuushallinta	vahvistus, tiedotus, varmistetut tunnistustiedot ja valtuudet

	tiedottaa, mikäli käyttäjää ja valtuuksia ei löytynyt.	
Istunnon luominen	Pääsynhallinta luo istunnon, joka hallitsee käyttäjän kokonaistilaa.	istunto luotu
Istunto	Käyttäjä on tunnistettu ja hän on kirjautuneena sisään.	istunnon tila aktiivinen
Pääsyn eväyksestä tiedottaminen	Pääsynhallintaprosessi ja käyttövaltuushallinta on evännyt pääsyn. Eväämisestä tiedotetaan käyttäjää tarvittaessa.	tiedotus
Pääsyn eväyksen vastaanottaminen	Käyttäjä vastaanottaa tiedon valtuuksien puuttumisesta.	vastaanotettu ilmoitus
Liittymäprosessit		
Federointi	Ulkoisen vahvan tunnistamisen ja tunnistamisen hallinta ulkoisessa järjestelmässä, tunnistamissanoman siirto kohdeorganisaation käyttöön.	
Vahvan tunnistamisen hallinta	Kunnan sisäisen vahvan tunnistamisen hallinta: onko hyväksyttävä tapa, onko oikea tunniste tai varmenne, tunnisteeseen liittyvien tietojen siirto.	vahva tunnistus tarkistettu
Kertakirjautuminen	Tunnistettu, hyväksytty käyttäjä hyväksytään kertakirjautumisen piiriin.	

8.5.5 Kertakirjautuminen

Kertakirjautuminen tarjoaa käyttäjälle yhdellä tunnistautumisella pääsyn useaan sovellukseen. Kertakirjautuminen ei poista järjestelmäkohtaisia käyttäjätunnuksia ja salasanoja.

-



Prosessi /tehtävä	Kuvaus	Tiedot/tulos
Käyttäjän tilatietojen tulkitseminen	Käyttäjän tilatietojen hallinta ja kohdejärjestelmän käyttäjätunnuksen ja salasanan haku salasanakukkarosta	käyttäjän kirjautumistiedot haettu
Tietojen välittäminen kohdejärjestelmään	Kertakirjautumisprosessi välittää käyttäjän tiedot (myös työroolin) kohdesovellukselle automaattisesti. (Työrooli sisältää myös palvelunkäyttäjien/ asiakkaiden roolituksen)	tunnistus ja kirjautumistiedot välitetty kohdejärjestelmälle
Tunnistautumistietojen vastaanottaminen	Kohdejärjestelmä vastaanottaa ja tarkistaa käyttäjän tunnistetiedot	
Sovellusistunnon perustaminen	Kohdejärjestelmä perustaa sovellusistunnon käyttäjälle tunnistustietojen perusteella	istunto perustettu käyttäjälle

8.5.6 Seuranta

Lokituksessa noudatetaan VAHTI 3/2009 –ohjeen mukaista ylläpitolokia. Ylläpitoloki sisältää lokitiedot:

- käyttöoikeuksien muutoksista, poistoista ja lisäyksistä
- rekistereiden käyttöön liittyvien virhetilanteiden hallinnasta
- järjestelmään tehdyistä muutoksista

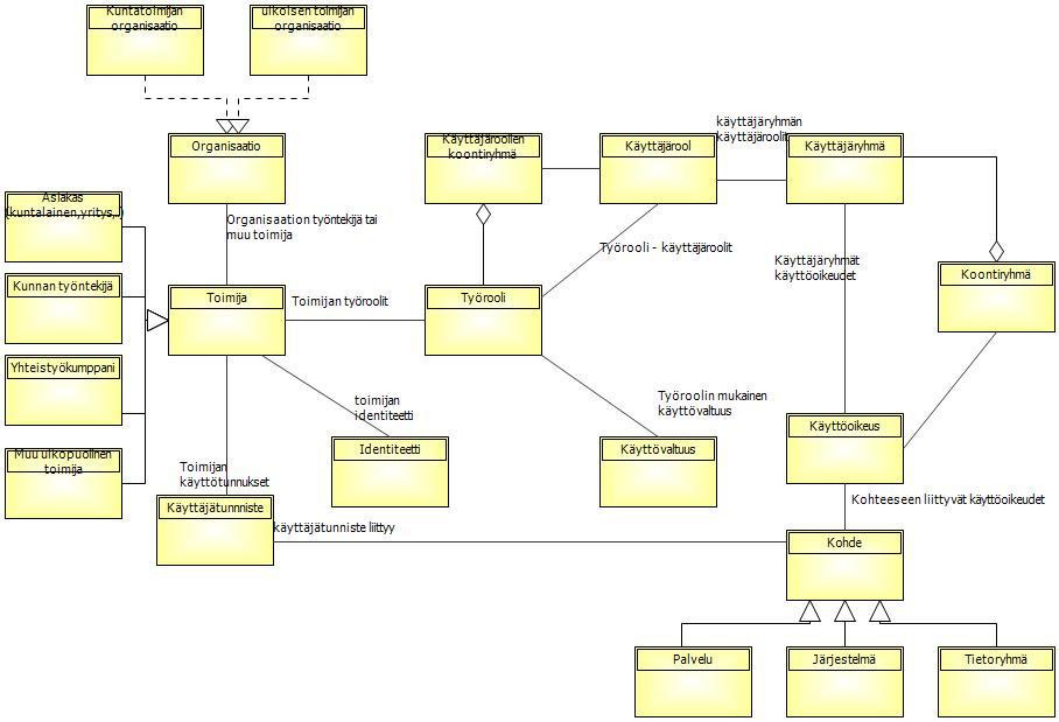
Myös itse lokia tulee seurata.

- Lokia ei saa voida muuttaa

9 Kuvattavan kohteen käsite- malli ja tietomalli

Tässä kappaleessa kuvataan käyttövaltuushallintaan liittyvät keskeiset peruskäsitteet ja käsitteiden väliset suhteet. Käsitemallissa on kuvattu työroolien yhteys käyttäjä-ryhmiin ja käyttöoikeuksiin.

Kuvatussa tietomallissa on otettu huomioon toimintalogiikan ja prosessien tarvitsemat ja tuottamat tiedot ylätasolla. Keskeiset tietomallit on kuvattu alla olevissa kappaleis-sa.

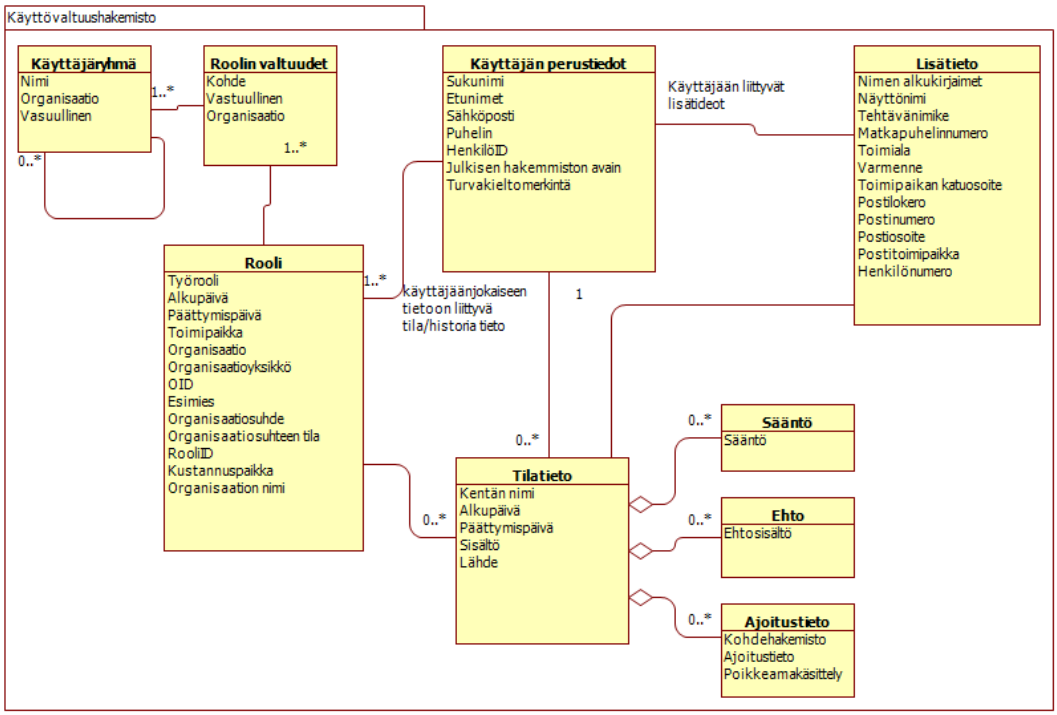


Kuva 14: Käsitemalli ylätasolla

Käsite	Kuvaus
Toimija (Käyttäjä)	Yksilö tai ryhmä, joka (päivittäin) käyttää järjestelmää sen oikeassa käyttöympäristössä (JHS 171). Tietojärjestelmäpalveluja käyttävä henkilö, ryhmä tai ohjel-misto (VAHTI_Liite4 sanasto). • Kunnan työntekijä • Yhteistyökumppani • Asiakas • Kuntalainen, henkilöasiakas • Yritys, yrityksen työntekijä

	• Muu ulkopuolinen toimija • Harjoittelija, opiskelija
Organisaatio	Toimijaan mahdollisesti liittyvä organisaatio (ei kuntalaisten yhteydessä tietoa), organisaatio, jossa toimija on työntekijänä • Kunnan työntekijä: kuntatoimijan organisaatio • Yhteistyökumppani, yritysasiakas, muu ulkopuolinen toimija: ulkoisen toimijan organisaatio
Käyttäjärooli	Käyttäjärooli voi olla käyttäjä (ihminen) tai toinen tietojärjestelmä (JHS 171). Käyttäjäroolia tarkastellaan palvelujärjestelmissä olevien valtuuksien näkökulmasta (VAHTI sanasto). Käyttäjäroolit määritellään käyttäjäryhmittäin.
Käyttäjätunniste	Toimijan käyttäjätunnus ja salasana/varmenne+ PIN hänelle valtuutettuihin eri kohteisiin (palveluihin tai järjestelmiin
Työrooli (business role)	Käyttäjän toimenkuvaan hänen työorganisaatiossaan kuuluvat työroolit ja työroolin mukaiset toimintavaltuudet sekä laajennettuna myös asiakkaisiin/asiakkaiden puolesta asioijien työroolin mukaiset valtuudet
Käyttäjäryhmät (user groups	Järjestelmien, tuotteiden tai palveluiden käyttäjäkunta jaetaan sopiviin käyttäjäryhmiin. Käyttäjäryhmät on toteutettu yleensä järjestelmä-, sovellus- tai tuotekohtaisesti. Yhtä yhteistä tapaa käyttäjäryhmien toteuttamiseen ei ole olemassa. Käyttäjäryhmiin liitettävät käyttäjäroolit määritellään käyttäjäryhmittäin.
Identiteetti	Käyttäjän/toimijan yksilöivä tunniste, joka on pakollinen käyttäjäkohtaisten tai personoitujen verkkopalvelujen, kertakirjautumisen ja luottamusverkostojen hallinnassa.
Käyttövaltuus	Toimijalle (tietojärjestelmän käyttäjälle) tai tietyn työroolin omaavalle käyttäjäryhmälle myönnetyt yksilöidyt oikeudet nimettyjen palveluelementtien tai muiden resurssien käyttöön. Käyttövaltuudet määrittelevät, miten ja millaisilla edellytyksillä käyttäjällä on oikeus käyttää ao. palveluelementtejä.
Käyttöoikeus	Kohteeseen liittyvät käyttöoikeudet, jotka on myönnetty eri käyttäjäryhmille.
Kohde	Kohde on tarkasteltava kokonaisuus jolle on määritelty käyttöoikeudet.

9.1 Käyttövaltuushakemiston tietomalli

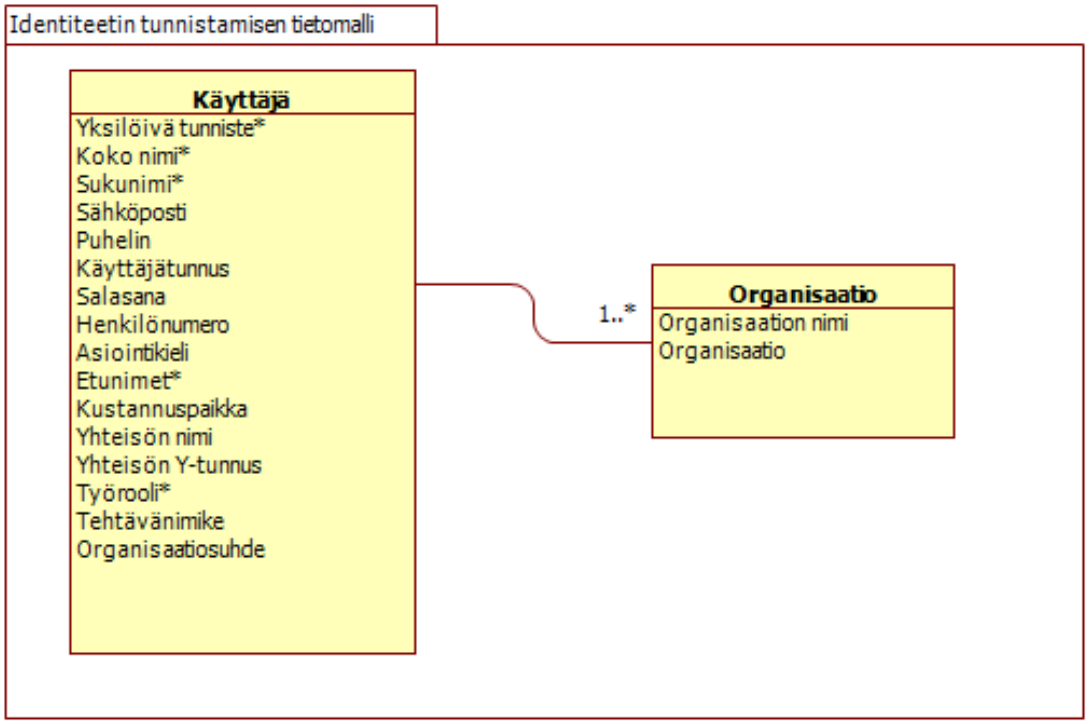


Kuva 15: Käyttövaltuushakemiston tietomalli

Tieto	Kuvaus
Käyttäjän perustiedot	Käyttäjään liittyvät perustiedot: • Sukunimi • Etunimet • Sähköposti: Sähköpostiosoite (työntekijä master datan mukaisesti) • Puhelin: Puhelinnumero muodossa +358.. • HenkilöID (Personal ID- P.ID): Käyttäjän yksilöivä tunniste (11 digittiä) • Julkisen hakemiston avain: Avain kryptaukseen tai kryptauksen purkamiseen • Turvakieltomerkintä: Tietojenluovutuskielto. Merkintä kertoo, että henkilöllä on Väestötietojärjestelmässä tietojenluovutuskielto, joka koskee henkilön kotikuntaa ja osoitteita. Rekisterinpitäjällä on erityinen velvollisuus varmistaa turvakiellon toteutuminen.
Lisätieto	Käyttäjään liittyvät tarvittavat lisätiedot, voivat vaihdella hakemistoittain. Lisätiedot eivät ole pakollisia. • Henkilönumero: Henkilöstö master datassa määritelty attribuutti, joka luodaan henkilöstöhallinnossa henkilön tietojen kirjaamisen yhteydessä – viite henkilöstöhallintoon
Rooli	Käyttäjään liittyvät työroolit ja roolin tiedot: • Työrooli, työroolin alku- ja päättymispäivä

	• Työrooliin liittyvä toimipaikka, sopimuksen mukainen organisaatio (ly-tunnus, D.U.N.S), organisaatioyksikkö, kustannuspaikka sekä organisaation nimi • Organisaation OID–koodi • Työrooliin liittyvä esimies • Organisaatiosuhde: Virka, työsuhteinen, määräaikainen, sijaisuus, ulkoinen, kuntalainen, .. • Organisaatiosuhteen tila: aktiivinen, pitkällä vapaalla, eronnut, passiivinen,… • RooliID (R.ID): roolin yksilöivä tunniste
Tilatieto	Kenttäkohtainen tilatieto, nykyinen ja tulevatila: Kentän nimi, johon tilatieto liittyy Alku ja loppuaika: tilan muutokseen liittyvä aika (tulevaisuus, arvo muuttuu) Sisältö: kentän sisältö – muutoksen yhteydessä Lähde: Lähdejärjestelmä, josta saadaan tilatieto eli mistä hakemistosta tieto tulee/on Sääntö: • Kertoo miten asioita tarkastellaan esim. mitkä ovat pakolliset tiedot mitä tietoja voidaan lähdehakemistoista päivittää, jne. Ehto: Liittymisehdot, hierarkiaehdot, jne. • Esim. käyttäjä luodaan joissakin hakemistoissa, kun vaadittavat tiedot ovat olemassa, roolin siirtoprosessiin liittyvät ehdot täyttyvät tai joissain hakemistossa päivitetään henkilön tila vapaalle pidemmän loman aikana, toisissa hakemistoissa ei tehdä mitään. Ajoitustieto: • Ajoitukseen liittyvät tiedot ja käsittelysäännöt, aikataulut • Esim. hakemistojen ajantasaistamisen päivitysaikataulut/ tiedonsiirtoaikataulut: kirjoitettava tietyn hakemistolle sopivan aikataulun mukaisesti, kirjoitukset on ryt-mitettävä.
Roolin valtuudet	Työroolin mukaiset oikeudet eri kohteisiin. • Kohde • Vastuullinen: kohteen omistaja/pääkäyttäjä • Organisaatio: kohteen omistava/ylläpitämä organisaatio
Käyttäjäryhmä	Kohteen käyttäjäryhmä, johon käyttäjä kuuluu. Käyttäjäryhmä voi koostua ryhmistä (koontiryhmä). Käyttäjäryhmästä vastaava (omistaja/pääkäyttäjä). Käyttäjäryhmän vastuuorganisaatio.

9.2 Identiteetin tunnistamisen tietomalli (”tiketti”)



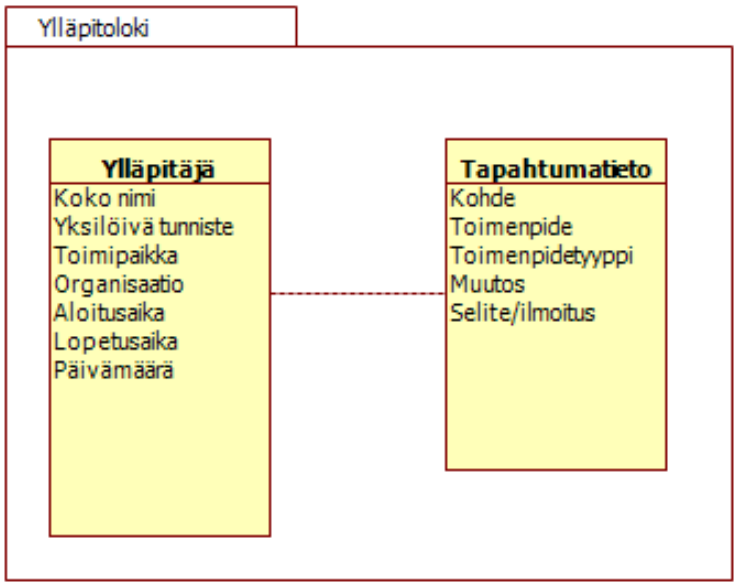
Kuva 16: Identiteetin/ tunnistusselosteen (”tiketin”) tietomalli

Käyttötilanteesta riippuu, mitä attribuutteja identiteettiin kulloinkin tarvitsee liittää. Muiden kuin tarpeellisten attribuuttien kerääminen ja tallettaminen henkilöstä kielletään henkilötietolaissa.

Tieto	Kuvaus
Käyttäjä	Käyttäjään/henkilöön liittyvät keskeisimmät tie-dot/attribuutit: • Yksilöivä tunniste* • Koko nimi • Sukunimi* • Sähköposti • Puhelin • Käyttäjätunnus • Salasana • Henkilönumero: työntekijän numero • Asiointikieli • Etunimet* • Kustannuspaikka: työroolin mukainen kustannuspaikka • Yhteisön nimi • Yhteisön Y-tunnus: esim. kun kyseessä on yritysasiakas • Työrooli*: käyttäjän työrooli, jossa asiointi tapahtuu

	• Tehtävänimike: käyttäjän henkilöstöhallinnon käyttämä tehtävänimike • Organisaatiosuhde: kuvaa käyttäjän suhteen organisaatioon (tunnistaneeseen organisaation)
Organisaatio	Organisaation tiedot voidaan määritellä useammalla hierarkisella rakenteella tai määritteellä • Organisaation nimi: organisaation selväkielinen nimi • Organisaatio: organisaation tunnus

9.3 Loki

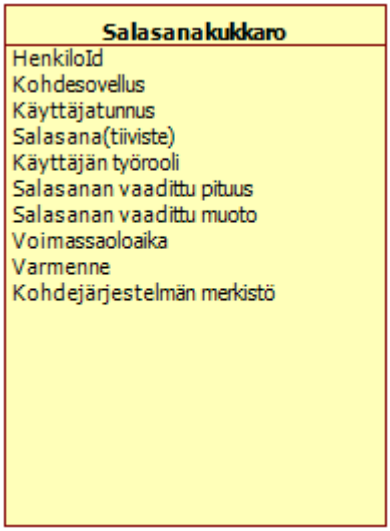


Kuva 17: Ylläpitolokin tietomalli

Tieto	Kuvaus
Ylläpitäjä	Ylläpitäjä: ylläpitäjään liittyvät keskeisimmät tiedot/attribuutit: • Koko nimi: Ylläpitäjän nimi • Yksilöivä tunniste: Lokiin kirjoittajan ID- tunniste, joka voi olla henkilön (personal) ID tai järjestelmän yksilöivä ID • Toimipaikka: Ylläpitäjän toimipaikka • Organisaatio: Ylläpitäjän organisaatio • Aloitusaika: Ylläpidon aloitusaika, (aikavyöhyke ja aika-formaatti pitää sopia) • Lopetusaika: Ylläpidon lopetusaika, (aikavyöhyke ja aika-formaatti pitää sopia) • Päivämäärä: Ylläpito/muutospäivä. (päivä-formaatti pitää sopia)
Tapahtumatieto	Tapahtumatieto, joka kuvaa ylläpitotapahtuman:

	• Kohde: ylläpidon kohde • Toimenpide: mikä lokitapahtuma/toimenpide on kysees-sä (esim. oliko kyseessä ylläpitotapahtuma) • Toimenpidetyyppi: tehdyn toimenpiteen tyyppi (esim. lisäys/poisto) • Muutos: mikä muutos tehtiin • Selite/Ilmoitus: perustelut, selite muutoksen syistä

9.4 Salasanakukkaro



Kuva 18: salasanakukkaron tietomalli

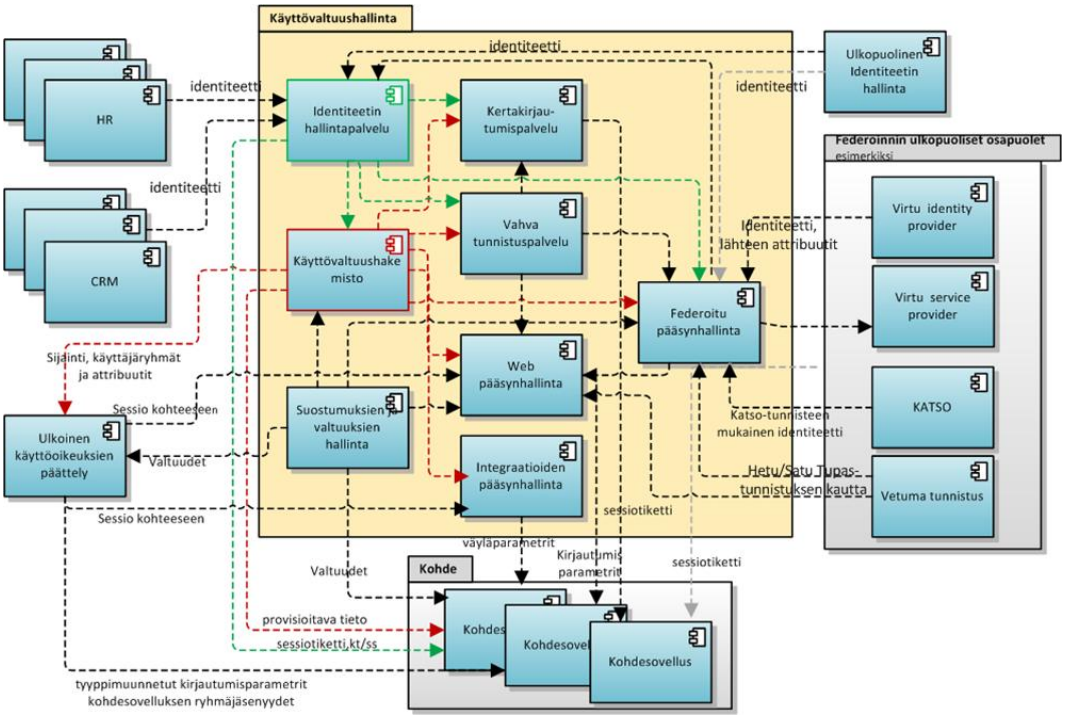
Tieto	Kuvaus
HenkilöId	Käyttäjän yksilöivä Id (tunnistusselosteessa ”tiketissä”)
Kohdesovellus	Kohdesovellus, johon käyttäjätunnukset ovat
Käyttäjätunnus	Käyttäjän käyttäjätunnus kohdesovellukseen
Salasana (tiiviste)	Käyttäjätunnukseen liittyvä salasana (tiiviste) kohdesovelluk-seen
Käyttäjän työrooli	Käyttäjän työrooli kohdesovelluksen suhteen
Salasanan vaadittu pituus	Kohdesovelluksen vaatima salasanan pituus
Salasanan vaadittu muoto	Kohdesovelluksen vaatima salasanan muoto, formaatti tai sääntö
Voimassaoloaika	Salasanan voimassaoloaika (alku-loppu)
Varmenne	Käyttäjätunnukseen - salasanaan liittyvä varmenne
Kohdesovelluksen mer-kistö	Kohdesovelluksen käyttämä merkistö (ASCII)

10 Järjestelmäarkkitehtuuri loogisella tasolla

10.1 Arkkitehtuurin sidokset muihin järjestelmiin

Tässä luvussa esitellään muutamia identiteetti- ja käyttövaltuushallintoon läheisesti liittyviä tietojärjestelmäpalveluita. Käyttövaltuushallinnalla on vahva sidos henkilöstönhallinta- ja asiakkaanhallintajärjestelmiin sekä master datan hallitaan.

Alla olevassa kuvassa on kuvattu keskeisimmät tietojärjestelmät ja tietojärjestelmäpalvelut, jotka liittyvät käyttövaltuushallintaan ja jotka tulee ottaa huomioon tapauskohtaisesti. Kuntaorganisaatiossa on tunnistettava ja sovellettava tarpeenmukaista ympäristöä.



Kuva 19: Arkkitehtuurin mukainen toimintaympäristö: järjestelmien väliset yhteydet

Perustiedon hallinta (MDM)

Perustiedon hallinnan tietojärjestelmäpalveluita tarvitaan, kun jollekin tietoryhmälle (esim. asiakastiedot) on olemassa useita tallennuspaikkoja ja halutaan tarjota yksi

eheä näkymä tähän tietoon. Käyttövaltuushallinnassa erityisesti identiteetinhallinta saattaa hyödyntää perustiedon hallinnan tietojärjestelmäpalveluita, jos nämä ovat olemassa esimerkiksi työntekijä-, asiakas- ja kumppanitietojen suhteen.

Henkilöstöhallinta (HRM)

Henkilöstöhallinnan tietojärjestelmäpalveluista saadaan työntekijöihin ja heidän työsuhteeseensa liittyviä tietoja, joita voidaan hyödyntää käyttäjien ja käyttövaltuuksien elinkaaren hallinnassa. HRM-järjestelmistä tulee pyrkiä tekemään integraatiot joko suoraan identiteetinhallintaan tai vaihtoehtoisesti tehdä ne perustiedonhallinnan kautta.

Asiakashallinta (CRM)

Asiakashallinnasta saadaan asiakkaisiin ja heidän edustamiin organisaatioihin liittyvää tietoa, jota voidaan hyödyntää käyttäjien ja käyttövaltuuksien elinkaaren hallinnassa. CRM-järjestelmistä voidaan tehdä joko suorat integraatiot identiteetinhallintaan tai vaihtoehtoisesti tehdä ne perustiedonhallinnan kautta.

Sähköinen allekirjoitus

Sähköisen allekirjoitus tarjoaa palvelut, joita tarvitaan sähköisten allekirjoituksien tuottamiseen sekä niiden alkuperän, aitouden, muuttamattomuuden yms. vaatimusten todentamiseen. Esimerkiksi kryptografisten allekirjoitusten käyttämät laatuvarmenteet yms. ovat monelta osin teknologisesti samoja ratkaisuita kuin vahvan tunnistuksen vaatimat ratkaisut. Esimerkiksi sama toimikortti voi sisältää sekä tunnistamisen että allekirjoittamisen vaatimat tiedot ja toiminnallisuudet. Sähköisen allekirjoituksen ja vahvan tunnistuksen väliltä löytyy synergioita.

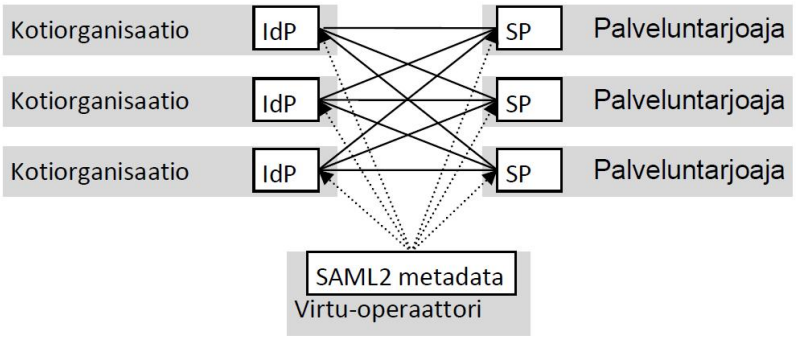
Sähköinen maksaminen

Sähköinen maksaminen tarjoaa palvelut, joita tarvitaan sähköisessä maksamisessa. Yhtenä esimerkkinä sähköisen maksamisen ratkaisuista on VETUMA-maksaminen. VETUMA-maksaminen nojaa samaan tekniseen ratkaisuun kuin VETUMA-tunnistus. Myös federoidun tunnistamisen ja sähköisen maksamisen välillä voi löytyä synergioita.

Virtu luottamusverkko

Virtussa identiteetin tarjoajana toimii käyttäjän kotiorganisaatio (virasto) ja palvelun-tarjoajana mikä tahansa luottamusverkkoon liittynyt toimija. Käyttäjän kotiorganisaatio voi toimia myös palveluntarjoajana niin omille kuin organisaation ulkopuolisillekin käyttäjille. Virtu-operaattorin roolina on toimia mm. luottamusverkon metatietojen ylläpitäjänä. Verkostoon kuuluvat palvelun tarjoajat luottavat identiteetin tarjoajien tekemään tunnistukseen ja niiden tarjoamiin käyttäjätietoihin. Toiminta perustuu SAML 2.0 mukaiseen identiteetin tarjoaja (IdP, Idenitity Provider) ja palvelun tarjoaja (SP, Service Provider) –toimintamalliin.

Alla on kuva Virtun osapuolista ja toimintamallista. (*Viite: kuva alla on Virtu-dokumentaatiosta.)*



Identiteetti ja käyttövaltuudet: Virtussa käyttäjän tunnisteena toimii käyttäjän kotiorganisaation tunnus yhdistettynä organisaation käyttämään käyttäjän yksilöivään tunnukseen. Käyttäjän attribuuteilla pystytään kuvaamaan käyttäjän perustietojen lisäksi niin käyttäjien rooleja kuin käyttöoikeuksiakin. Käyttäjätietojen attribuutteja voidaan tarvittaessa myös lisätä.

Käyttövaltuuksien hallintaa voidaan tehdä kolmella tavalla:

1. Käyttövaltuutta ylläpidetään kokonaan palvelussa
2. Käyttövaltuutta ylläpidetään kokonaan kotiorganisaatiossa ja käyttöoikeudet välitetään palvelulle käyttäjän attribuuteissa
3. Käyttövaltuus perustuu rooliin, jonka kotiorganisaatio ylläpitää ja ojentaa kirjautumishetkellä palveluun.

Vetuma tunnistus

Vetuma tarjoaa palvelut tunnistamiseen, hyväksymisen allekirjoittamiseen ja verkkomaksamiseen. Tunnistus tehdään pääasiassa pankkien TUPAS- tai VRK:n kansalasivarmennetunnistamisella, jolloin käyttäjien tietoja ei tarvitse ylläpitää asiointipalveluiden toimesta. Näissä tapauksissa tunnistustietoja voidaan täydentää VTJ:stä saatavilla tiedoilla. Asiointipalveluiden on myös mahdollista ylläpitää VETUMA-palvelussa omaa käyttäjärekisteriään, jolloin tunnistus voidaan tehdä myös käyttäjätunnuksella ja salasanalla.

Identiteetti ja käyttövaltuudet: VETUMA-palvelua voidaan käyttää käyttäjien tunnistamiseen. Käyttäjät identifioidaan aina henkilötunnuksella (HST-toimikorttia käytettäessä myös SATU:lla). Käyttövaltuuksia ja –rooleja ei voida tallentaa VETUMA:an, joten myös SAML v2.0 mukaisessa käytössä sen käyttötarkoitus on yksistään käyttäjän tunnistaminen. Käyttäjäroolit ja –valtuudet tulee aina toteuttaa kuhunkin käyttövaltuuksien hallintapalveluun.

KATSO

Katso-tunnistus on Verohallinnon tarjoama, yrityksiä varten luotu tapa tunnistautua viranomaisten sähköisiin palveluihin. Yritysten lisäksi Katso-tunnistusta voivat käyttää yhtymät, julkiset organisaatiot (esimerkiksi kunnat) ja kuolinpesät.

Organisaation Katso-tunnisteen eli pääkäyttäjyyden saa käyttöönsä henkilö, jolla on organisaation nimenkirjoitusoikeus (kaupparekisteriote). Pääkäyttäjyys voidaan myöntää kaikille, joilla on yrityksen nimenkirjoitusoikeus. Pääkäyttäjä voi luoda yrityksen työntekijöille Katso-alitunnisteita, joilla on Katso-tunnistetta rajoitetummat oikeudet. Katso-alitunnisteen voi myöhemmin muuntaa (vahventaa) Katso-tunnisteeksi sähköisen tai henkilökohtaisen tunnistamisen kautta. Pääkäyttäjä voi myös myöntää ja vastaanottaa valtuutuksia. Katso-tunnisteen omaavat käyttäjät voivat tunnistautua joko heikosti (käyttäjätunnus ja salasana) tai vahvasti (käyttäjätunnus, salasana ja kertakäyttösalasana listalta). Alitunnuksille on vain heikko tunnistus (käyttäjätunnus ja salasana).

KATSO-palvelu on toteutettu SAML v 2.0:lla – Ubisecuren tuotteilla. Katso-palvelu toimii identiteetin tarjoajana (IdP).

Identiteetti ja käyttövaltuudet: Katso-tunnisteisiin liitetään aina henkilön henkilötunnus. Katso-alitunnisteisiin ei liitetä koskaan henkilötunnusta. Asiointipalvelut voivat hakea käyttäjän roolitiedot roolikyselyllä.

Näin ollen asiointipalvelut voivat hallita käyttövaltuuksia kahdella tavalla:

- Käyttövaltuutta ylläpidetään kokonaan palvelussa
- Käyttövaltuus perustuu rooliin, jota kunkin tunnistettavan organisaation pääkäyttäjät ylläpitävät ja jonka KATSO-palvelu ojentaa kirjautumisen jälkeen asiointipalvelulle roolikyselyssä. Asiointipalveluiden omistajat voivat pyytää uusia roolityyppejä lisättäväksi KATSO-palveluun.

Ulkopuolinen Identiteetin hallinta

Ulkopuolinen identiteetin hallinta tunnistaa käyttäjän ja käyttäjän valtuudet. Käyttäjä on luotu ulkopuoliseen identiteetin hallintajärjestelmään

1. Organisaation identiteetin hallinta provisioi ulkopuolelle tunnistautuneen roolin valtuudet kohdejärjestelmään
2. Osaoptimointitoteutuksessa ulkopuolinen identiteetti voidaan kuljettaa (federoitu pääsynhallinta) yksittäiseen sovellukseen käyttövaltuuksien osan tai kertakirjautumisen avulla. Tällä menettelyllä ratkaistaan yksittäinen sovellustarve, jossa siirretään ongelma toiseen kohtaan.

(katso Liite 1 Esimerkkiskenaariot)

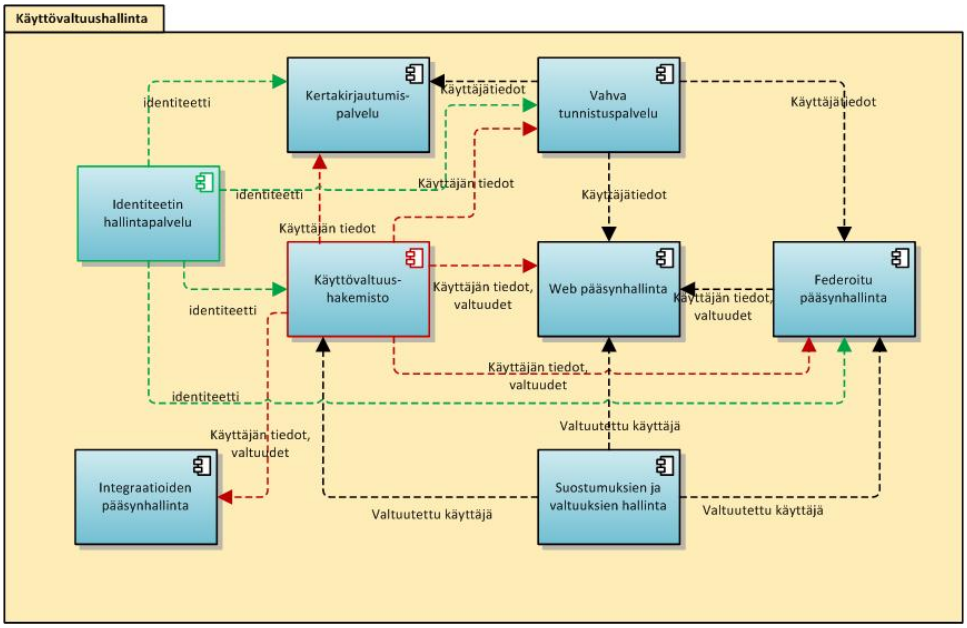
Ulkoinen käyttöoikeuksien päättely

Ulkoinen käyttöoikeuksien päättely mahdollistaa käyttövaltuuksien tarkastamisen sovelluksen tai palvelun ulkopuolella. Perinteisen sovelluksen sisään rakennettavan päättelyn sijaan sovellus kutsuu ulkoista käyttöoikeuksien päättelyä (esim. tämä käyttäjä haluaa tehdä tällaisen toiminnon tällaiselle objektille), johon käyttöoikeuksien päättely vastaa voidaanko toiminto sallia kyseiselle käyttäjälle (esim. kyllä / ei / en tiedä).

(katso Liite 1 Esimerkkiskenaariot)

10.2 Arkkitehtuurin osat, osien sidokset

Tässä luvussa kuvataan viitearkkitehtuurin kohdearkkitehtuurin jakautuminen toiminnallisiin osakokonaisuuksiin karkealla tasolla.



Kuva 20: käyttövaltuushallinnan osat, palvelukomponentit

Identiteetin hallintapalvelu

Identiteetin hallinta vastaa käyttäjien ja käyttövaltuuksien hallinnasta ja niihin liittyvistä prosesseista työsuhteen koko elinkaaren ajan (aloittaa työt, vaihtaa työtehtäviä, lopettaa työt). Identiteetin hallinnan avulla käyttäjät voivat hakea tai käyttäjille voidaan hakea ja hyväksyä käyttövaltuuksia. Myönnetyt käyttövaltuudet provisioidaan kohdejärjestelmiin ja hakemistoihin automaattisesti tai manuaalisesti. Automaattinen provisiointi tarkoittaa käyttäjän tai käyttövaltuuksien automatisoitua perustamista tai poistamista. Manuaalinen provisiointi puolestaan tarkoittaa samojen tietojen ylläpitoa ihmiskäyttäjän toimesta (esim. ylläpitäjä tai pääkäyttäjä). Identiteetinhallinta pitää kirjaa millaisia oikeuksia kullakin käyttäjällä oli kunakin ajanhetkenä sekä valvoo ja auttaa löytämään ns. vaarallisia työyhdistelmiä. Käyttövaltuuksien hallinnassa hyödynnetään työ- ja järjestelmärooleja. Työroolit kuvaavat tehtäviä, joita ihmiset tekevät, esimerkiksi esimies, kirjanpito jne. Järjestelmäroolit puolestaan vastaavat eri järjestelmien sisältämiä käyttövaltuuksia. Kullekin työroolille määritellään ne järjestelmäroolit, joita kyseisten tehtävien suorittamiseksi tarvitaan. Identiteetinhallinta sisältää usein myös itsepalvelutoiminnallisuuksia mm. salasanojen palauttamiseen jne. Huom! Käyttäjä- ja käyttövaltuustietoja ei haeta koskaan identiteetin hallinnasta, vaan joko hakemistoista tai kohdesovelluksista itsestään.

Käyttövaltuushakemisto

Käyttäjä- ja käyttövaltuushakemistot ovat keskeisimpiä identiteetinhallinnan provisiointikohteita. Sovellukset ja pääsyhallinnasta vastaavat tietojärjestelmäpalvelut käyttävät hakemistoja sekä käyttäjien tunnistamiseen (autentikointi) että käyttövaltuuksien tarkastamiseen (autorisointi).

Kertakirjautumispalvelu

Kertakirjautuminen tarjoaa käyttäjälle yhdellä tunnistautumisella pääsyn useaan sovellukseen. Kertakirjautumisen tietojärjestelmäpalvelu ei poista sovelluskohtaisia käyttäjätunnuksia ja salasanoja, vaan poistaa käyttäjän sisäänkirjautumistarpeen tallentamalla käyttäjän käyttäjätunnukset ja salasanat talteen ja syöttämällä ne käyttäjän puolesta kohdesovellukselle. Kertakirjautumisratkaisut pystyvät integroitumaan erilaisilla teknologioilla toteutettuihin käyttöliittymiin (esim. Windows-, Java- ja web-sovellukset sekä pääte-emulaattorilla käytettävät käyttöliittymät jne.) Kertakirjautumisratkaisu voi tarjota myös ns. kioski-moodin, jossa useampi käyttäjä käyttää samaa päätelaitetta vuorotellen. Tavoitteena on mahdollisimman nopea sisäänkirjautuminen usein toimikortin avulla (ks. myös vahva tunnistus -tietojärjestelmäpalvelu). Käyttäjä pystyy jatkamaan toimiaan samasta tilanteesta siirtyessään kioski-päätelaitteelta toiselle.

Vahva tunnistuspalvelu

Vahva tunnistus –tietojärjestelmäpalvelu huolehtii käyttäjän vahvasta tunnistuksesta. Vahvassa tunnistuksessa käytetään kahta tunnistusmenetelmää seuraavasta kolmesta eli jotain, jota

1. käyttäjä tietää
2. käyttäjällä on
3. käyttäjä on.

Web-pääsynhallinta

Web-pääsynhallinta suorittaa web-sovellusten pääsyn kontrolloinnin eli käyttäjän tunnistamisen ja valtuutuksen käyttövaltuuksien mukaisesti (sisäänpääsyn tai eston). Web-pääsynhallinta vastaa ns. karkean tason pääsynhallinnasta. Pääsynhallinnan lisäksi se tarjoaa siihen integroitujen web-sovellusten yli menevän yhdistetyn käyttäjäistunnonhallinnan. Näin yhdellä kertakirjautumisella käyttäjä pääsee käyttämään kaikkia kertakirjautumisen piirissä olevia sovelluksia. Web-pääsynhallinnan suorittaa tunnistuksen ja valtuutuksen hakemistoja vasten. Tunnistuksessa voidaan hyödyntää myös vahvaa tunnistusta.

Federoitu pääsynhallinta

Federoitu pääsynhallinta perustuu usein luottamusverkkoon, joka muodostuu tyypillisesti identiteetin tarjoajista ja palveluiden tarjoajista. Käyttäjä tunnistautuu jossain verkoston identiteetin tarjoajassa, jonka jälkeen palveluntarjoajat eivät enää vaadi häntä tunnistautumaan uudelleen, vaan luottavat alkuperäiseen tunnistukseen ja käyttävät sitä käyttövaltuuspäätöksissään. Federoitu pääsynhallinta – tietojärjestelmäpalvelu sisältää identiteetin tarjontaan ja palveluntarjontaan liittyvät tunnistuspalvelut ja tiedon välittämisen sekä luottamusverkoston tietojen ylläpitoon

liittyvät toiminnot. Federoitu pääsynhallinta tarjoaa myös federoidun verkoston keskitetyn ”käyttäjäistunnon”. Näin federoitu pääsynhallinta tarjoaa organisaatiorajat ylittävän kertakirjautumisen. Tämä on merkittävä ero verrattuna kertakirjautumisratkaisuihin tai web-pääsynhallinnan ratkaisuihin. Federoitu pääsynhallinta toimii usein yhdessä web-pääsynhallinnan kanssa tarjoten yhtenäisen ratkaisun sekä organisaation omaan että organisaatiorajat ylittävään kertakirjautumiseen.

Suostumusten ja valtuutuksien hallinta

Suostumusten ja valtuutuksien hallinta täydentää käyttäjä- ja käyttövaltuushakemistojen tietoa kertomalla käyttäjille mahdollisesti myönnetyistä erityisistä suostumuksista tai valtuutuksista hoitaa toisten asioita, esimerkiksi holhoojan valtakirjasta hoitaa holhottavan asioita.

Palveluiden ja integraatioiden pääsynhallinta

Palveluiden ja integraatioiden pääsynhallinta suojaa julkaistuja palveluita ja sovellusintegraatioita asiattomilta käyttäjiltä. Tunnistukseen saatetaan käyttää ns. teknisiä tunnuksia. Teknisten tunnusten sijaan voidaan käyttää myös palvelukutsutunnistusta tai viestikohtaista loppukäyttäjätunnistusta ja käyttövaltuuksien tarkastamista.

Ulkoinen käyttöoikeuksien päättely

Ulkoinen käyttöoikeuksien päättely mahdollistaa käyttövaltuuksien tarkastamisen sovelluksen tai palvelun ulkopuolella. Perinteisen sovelluksen sisään rakennettavan päättelyn sijaan sovellus kutsuu ulkoista käyttöoikeuksien päättelyä (esim. tämä käyttäjä haluaa tehdä tällaisen toiminnon tällaiselle objektille), johon käyttöoikeuksien päättely vastaa voidaanko toiminto sallia kyseiselle käyttäjälle (esim. kyllä / ei / en tiedä).

Osien toimintaa on kuvattu tarkemmin esimerkkiskenaarioissa katso Liite 1.

11 Arkkitehtuurin käyttämät standardit ja yleiset määritelmät

Käyttövaltuushallinnan (KVH)-tietojärjestelmäpalveluiden välisessä kommunikoinnissa tulee nojata mahdollisimman pitkälle yleisiin käytössä oleviin standardeihin. Jokaisen vaadittavan standardin suhteen tulisi käydä läpi seuraava standardin elinkaari -analyysi ainakin nopeasti. Ennen standardin vaatimista tulee selvittää:

- miten laajalti standardi on käytössä

- mikä oletettavasti tulee olemaan standardin kohtalo pitkällä tähtäimellä.

Kuolevien ja vain muutamien tuotteiden tukemien standardien sijaan voidaan yhtä hyvin käyttää myös proprietary-rajapintoja tietojärjestelmäpalveluiden välillä.

Objektitason käyttövaltuudet tallennetaan objektin metatietoihin samaan paikkaan, jonne objektin muutkin metatiedot tallennetaan. Jos tämä ei ole mahdollista, objektitason oikeudet tallennetaan käyttäjä- ja käyttövaltuushakemistoon. Tulee tehdä kaikki mahdollinen, että jälkimmäistä vaihtoehtoa ei jouduttaisi käyttämään.

Alla on suosituksen omaisesti lueteltu teknisen arkkitehtuurin osalta yleisiä käyttövaltuushallintaan liitettyjä ja hyväksyttyjä standardeja.

Standardit, menetelmät ja määritelmät	Toimialue/ protokolla	Lyhyt kuvaus
LDAP	Lightweight Directory Access Protocol	LDAP on hakemistopalvelujen käyttöön tarkoitettu verkkoprotokolla. LDAP:in yleisin käyttötarkoitus on käyttäjäntunnistus ja käyttöoikeuksien tarkistaminen. Henkilötietomalli LDAP- hakemistolle http://schema.org/Person
Microsoft Windows Active Directory Schema		Microsoftin aktiivihakemisto koostuu yhdestä tai useammasta toimialueesta (domain). Toimialueiden niminä käytetään DNS-nimiä. Metsä on yhden tai useamman yhtyeen liitetyn toimialueen kokonaisuus. Metsässä on yhteistä mm. seuraavat asiat: • Schema eli hakemistopalvelun rakenne • Global Catalog eli hakemiston hakupalvelu • aktiivihakemiston konfiguraatio
Kerberos (RFC 1964)	Todennus /Autentikointi protokolla	Kerberos on verkoston laitteiden autentikointiin liittyvä todentamispalvelu. Jotta Kerberos todentamispalvelu toimisi kunnolla, täytyy toimialueen koneiden kellojen olla tarkasti samassa ajassa.
NTLM (NT lan manager)	Tietoturva protokolla	NTLM on Microsoftin turvaprotokollaratkaisu, joka hoitaa istunnon autentikoinnin, luottamuksellisuuden ja eheyden käyttäjille.
Smart Card (ISO 7816, 14443)	Kortti protokolla	Smart Card voi tuottaa identiteetin, autentikoinnin ja prosessoinnin tunnisteiden avulla sekä toimii tietovarastona esimerkiksi salausavaimil-

Standardit, menetelmät ja määritelmät	Toimialue/ protokolla	Lyhyt kuvaus
		le.
OpenID	Tunnistautumis protokolla	OpenID tarjoaa vain käyttäjän tunnistautumisen. Tunnistautumisprotokollaa käytettäessä käyttäjälle palautetaan tunnistautumispalvelun allekirjoittama valtuutustieto, joka vahvistaa käyttäjän identiteetin.
PKI		PKI on julkisen avaimen hallintajärjestelmä. Se perustuu epäsymmetristen avainparien hallintaan luottamusverkossa. Rakenne voi olla sisäinen tai julkinen.
XACML	eXtensible Access Control Markup Language	XACML on tarkoitettu roolipohjaiseen käyttöoikeuksien hallintaan. Sen avulla voidaan määritellä käyttöoikeuksia erilaisille resursseille. XACML kertoo resurssikohtaisesti, mitä ja miten kukin käyttäjä (rooli) saa palvelua käyttää.
GeoXACML	Geospatial eXtensible Access Control Markup Language	GeoXACML on OGC:n tekemä laajennus XACML-standardiin. Se määrittelee geometrian yhtenä käyttöoikeuden rajoittamisen tai sallimisen tietotyyppinä ja tarjoaa erilaisia sijaintioperaattoreita maantieteellisten rajausten tekemiseen. GeoXACML:n avulla palveluun voidaan määritellä alueellisia rajoituksia (esim. Uusimaa), kohdeluokkien rajoituksia (esim. rakennukset) ja kohdekohtaisia rajoituksia (esim. tehdasrakennus). Roolinsa perusteella käyttäjä joko saa kohteiden tiedot tai ei saa niitä.
OAuth RFC 5849	Pääsynhallinta-protokolla	OAuth on avoin pääsynvalvontaprotokolla hajautetuille web-sovelluksille. Se mahdollistaa käyttäjien resurssien jakamisen palveluiden välillä ilman käyttäjätunnuksen tai salasanan luovuttamista kolmansille osapuolille.
SAML 2.0	Security Assertion Markup Language Tunnistautumis protokolla	SAML 2.0 on OASIS-komitean määrittelemä XML-pohjainen avoin standardi tunnistautumiseen ja pääsynhallintaan SAML määrittelee XML-pohjaiset työkalut tunnistautumisen ja pääsynhallinnan toteuttamiseksi. Varsinainen toteutus (esimerkiksi se, mitä tietoja siirretään ja millä tavalla) jätetään SAML:ssä toteuttajan päätettäväksi Varsinaiset SAMLviestit voivat kulkea synkronisesti esimerkiksi SOAP- tai HTTP-protokollilla
HAKA -> tama on luottamus-	Käyttäjien tunnistusjärjestel-	Haka on Suomen käytetyin korkeakoulujen ja tutkimuslaitosten käyttäjätunnistusjärjestelmä.

Standardit, menetelmät ja määritelmät	Toimialue/ protokolla	Lyhyt kuvaus
verkko, siirretään seurattaviin.	mä (Identity federation)	Myös käyttäjien henkilötietoja voidaan siirtää turvallisesti palveluihin kirjautumisen yhteydessä. Haka on yhteensopiva muiden pohjoismaiden korkeakoulujen luottamusverkostojen kanssa, joten käytettävissäsi ovat myös pohjoismaiset palvelut. Kotiorganisaation tietohallinto vastaa käyttäjiensä käyttäjätiedoista ja henkilöllisyyden todentamisesta. Hakassa olevien palvelujen käyttäjätiedot saadaan suoraan käyttäjän kotiorganisaatiosta
Federointi, valtuuksien välitys	Luottamusverkko hakemistojen välillä, esim. Saml2	Luottamisverkko luodaan joko kahden tai useamman operaattorin väliseksi tai laajemmaksi verkostoksi, jossa luotetaan alkuperäisen identiteetin haltijan tunnistamismenetelmiin ja annetaan siihen perustuva käyttövaltuus kohdehakemistosta. Valtuuksien välityksen yhteydessä voidaan lähettää ja ottaa vastaan valinnan mukaan käyttäjän kotihakemiston attribuuttitieto

12 Liitteet

Liite 1 Esimerkkiskenaariot

Liite 2 Tiedonsiirron periaatteet ja aikakaaviot

Liite 3 Käyttäjärooli- työrooli matriisi esimerkki

Liite 4 Etenemissuunnitelma

Liite 5 Sanasto

Liite 1

Kuntasektorin arkkitehtuuriryhmä

Kuntasektorin käyttövaltuushallinnan viitearkkitehtuuri

Versio 1.0

Pääsynhallinta, provisiointi, tunnistautuminen ja kertakirjautuminen esimerkkiskenaarioita

Helsinki 2013

Kuntaliitto
Kommunförbundet

Sisältö

Johdanto

Tämä kuvaus on tarkoitettu käytettäväksi ohjeena mietittäessä kunnan toimintaan sopivia toimintamalleja kertakirjautumisen ja pääsynhallinnan sekä federoinnin ratkaisua tunnistettaessa.
Tavoitteena on tyyppitapauskuvausten avulla auttaa kuntaa tunnistamaan omaan ympäristöönsä sopivat vaihtoehtoiset toimintamallit.
Kuvaus on toteutettu liitteeksi kuntasektorin käyttövaltuushallinnan viitearkkitehtuuriin.

Taustaa

2.1 Lähtökohdat

Käyttövaltuushallinnan- KVH (IAM) -palvelun avulla kunnat voivat hallita käyttäjä- ja käyttövaltuustohallinnon prosesseja ja pienentää merkittävästi näihin käytettävää työmäärää organisaation eri osissa
Palvelun avulla:

- voidaan jakaa ja monistaa käyttäjähallinnan pääprosesseja ja roolimalleja
- voidaan toteuttaa korkean käytettävyyden käyttäjähakemisto jaetuin kustannuksin
- mahdollistetaan kustannustehokkaasti myös pienille kunnille 24/7-palvelu käyttäjähallinnan keskeisille komponenteille yhteisestä valvontapisteestä
- saadaan kuntatoimialalle yhtenäinen käyttäjävaltuuksien jakelutapa, mikä tehostaa uusien sovellusten hankintaa ja liittämistä

Käyttövaltuushallinta- (IAM) muodostuu osakokonaisuuksista (erillisistä järjestelmäpalveluista):
eSSO- – kertakirjautuminen, enterprice Single Sign On

- kertakirjautuminen sovelluksiin hallitaan palvelun avulla
- ei muutoksia käyttäjähallintaan

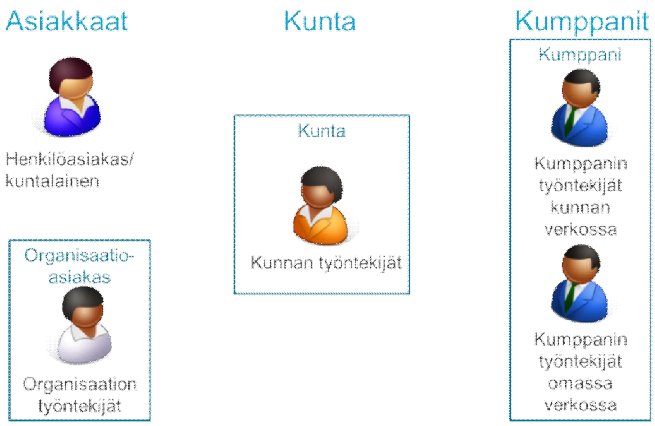
IdM– identiteetinhallinta, Identity Management

- tietojen synkronointi järjestelmien välillä
- käyttäjien aktivointi ja liittäminen palveluun
- hyväksymisprosessit ja valtuutus
- liittyminen ulkoisiin hakemistoihin

2.2 Käyttäjät /Roolit ylätasolla

Karkealla tasolla kunta ja sen ympärillä toimivat tahot ja käyttäjät (kuva alla) voidaan jakaa seuraaviin ryhmiin:

1. Asiakkaat:
    - henkilöasiakkaat,
    - Organisatioasiakkaisiin / sen työntekijöihin
2. Kunta
    - kunnan sisäiset työntekijät
3. Kumppanit
    - kumppanin työntekijät kunnan verkossa
    - kumppanin työntekijät omassa verkossaan



Kuva x: Kunnan ympärillä toimivat käyttäjät karkeasti ryhmiteltynä.

Ryhmä	Käyttäjä	Kuvaus
Asiakkaat	henkilöasiakas	Kunnan kanssa asioiva tai asioita hoitava/puolesta asioiva henkilö: • kuntalainen • ei-kuntalainen • jne.
	Organisaatioasiakas	Kunnan kanssa asioiva/asioita hoitavan organisaation työntekijä/jäsen. Organisaatioita voivat olla esimerkiksi • urheiluseurat • rakennusliikkeet, • mikä tahansa yritys tai yhdistys jne.
Kunta	Kunnan työntekijä	kunnan työntekijä: • kunnan virkamies • työsuhteinen työtekijä jne.)
	Muu kunnan toimija	Kunnan muu edustaja: • luottamushenkilö jne. kunnan käyttöoikeusverkkoa hyödyntävän organisaation työntekijät/jäsenet: • oppilas • tytäryhtiön työntekijä jne.
Kumppanit	Kumppanin työnteki-	Kunnalle tai kunnan puolesta palveluita tarjoavan/tuottavan organisaation työntekijä/jäsen, joka käyttää näiden tehtävien hoitamiseen kun-

	jä kunnan verkossa	nan käyttöoikeusverkkoa. Esimerkiksi: • vuokratyövoima • keikkalääkäri • räätälisovelluksen kehittäjä jne. Tällainen kumppanin työntekijä hyödyntää usein runsaasti kunnan tarjoamia tietojärjestelmäpalveluita.
	Kumppanin työnteki- jä omassa verkos- saan	Kunnalle tai kunnan puolesta palveluita tarjoavan/tuottavan organisaation työntekijä/jäsen, joka käyttää näiden tehtävien hoitamiseen pääasiassa oman organisaationsa käyttöoikeusverkkoa. Tällaisia kumppaneita voivat olla esimerkiksi • yksityinen päiväkoti • yleishyödyllisen organisaation hoitokoti • ruokapalveluita tuotava yritys • tietojärjestelmätoimittajan pääkäyttäjä jne. Tällainen kumppanin työntekijä hyödyntää yleensä kunnan tarjoamia tietojärjestelmäpalveluita vain vähäisissä määrin.

Toimintamalliskenaariot

Tässä luvussa on kuvattu tärkeimpiä käyttövaltuushallintaan kuuluvia tyyppitapauksia sekä erilaisia toimintamalleja, joilla tyyppitapauksen tavoitteisiin päästään. Kuvaukset selventävät tietojärjestelmäpalveluiden välisiä vastuita kuvaamalla niiden välillä kulkevat tietovirrat. Tyyppitapausten ja erilaisten toimintatapojen luettelot eivät ole kumpikaan tyhjentävän kattavia, mutta ne pyrkivät tuomaan esille ainakin keskeisimpiä vaihtoehtoja jatkokeskusteluiden ja -työn pohjaksi.
Tyyppitapauksissa esiintyvät tietojärjestelmäpalvelut voivat olla millä tahansa tavalla toteutettu. Esimerkiksi ”kunnan käytössä oleva käyttövaltuuksien ja identiteetinhallinta” voi olla kunnan omistama ja ylläpitämä tietojärjestelmäpalvelu tai kunnan palveluna ostama tietojärjestelmäpalvelu.

Kunnan työntekijät ja Kumppanin työtekijät kunnan verkossa
Tässä luvussa termillä työntekijä tarkoitetaan kahta käyttäjäryhmää:
- kunnan työntekijöitä
- kumppanin työntekijöitä kunnan verkossa.

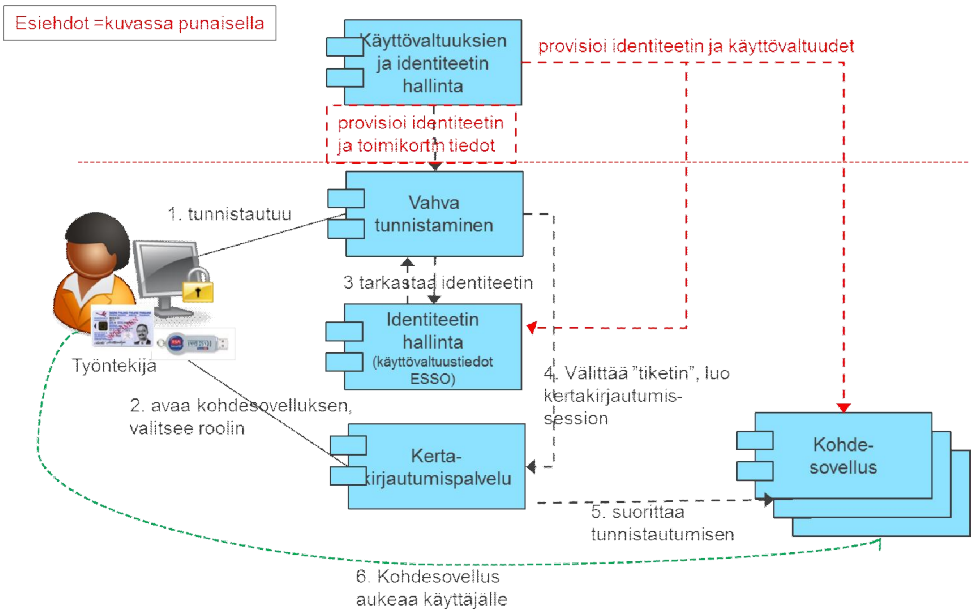
Federoiduissa toimintamalleissa Identity providerit, Service Providerit on esitetty selvyyden vuoksi yksinkertaisimman mallin mukaisina eli ne ovat kaikki kunnan käyttöönsä hankkimia (ostamalla tai palveluna).
Kun ryhdytään käyttämään ulkopuolisia Identity ja Service providereita toimintamallit muuttuvat samanlaisiksi kuin asiakaskäyttäjien tyyppitapauksissa on kuvattu.

3.1 Kunnan työntekijät ja kumppanit kunnan verkossa

Työntekijä kertakirjautuu sovellukseen

Tavoitteena kertakirjautuminen. Kertakirjautuminen edellyttää puolestaan vahvaa tunnistusta. Vahvan tunnistuksen tavoista toimikortit ovat ensisijainen ratkaisu. Toimikortilla tunnistetaan käyttäjä. Käyttäjälle on annettu oikeudet. Käyttäjälle voidaan myöntää myös väliaikainen toimikortti, jolloin käyttäjän tunnistus voidaan tehdä väliaikaisella toimikortilla. Juuri väliaikaisten toimikorttien takia käyttäjä pitää pystyä tunnistamaan usealla eri tavalla ja käyttövaltuuksien tulee olla ripustettuna käyttäjään – ei toimikorttiin.

3.1.1 Kertakirjautuminen kertakirjautumistietojärjestelmäpalvelun (ESSO) avulla



Kuva x: Työntekijä kertakirjautuu sovellukseen kertakirjautumisjärjestelmäpalvelun kautta (eSSO)

Esiehdot:

Työntekijän käyttövaltuudet ja identiteetti on provisioitu käyttövaltuuksien hallinnasta (luvitusprosessi) kertakirjautumistietojärjestelmäpalveluun sekä kohdejärjestelmiin. Käyttäjän identiteetti ja toimikortin tiedot on provisioitu vahvan tunnistuksen tietojärjestelmäpalveluun.

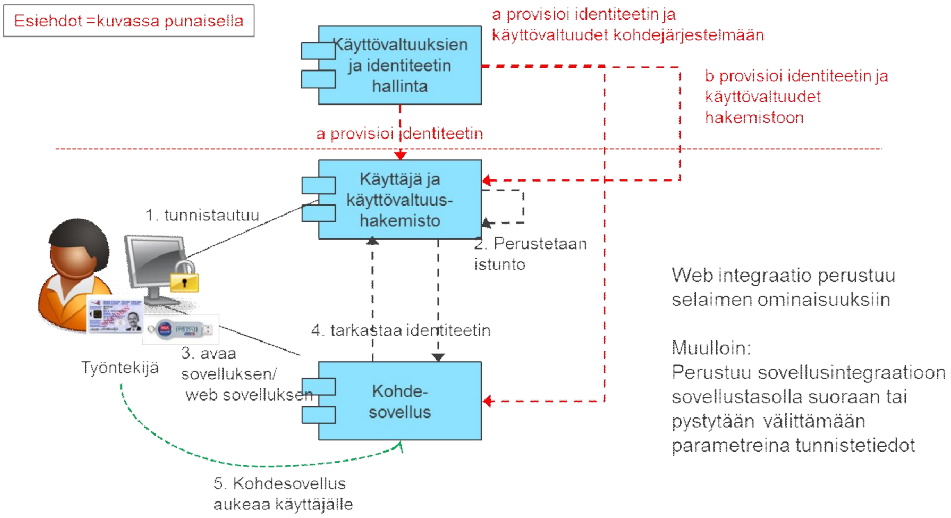
1. Käyttäjä tunnistautuu vahvasti ja vahva tunnistus tarkastaa käyttäjän tunnistautumisen valittua tunnistautumistapaa vasten ja välittää käyttäjän tiedot identifiointipalvelulle.
2. Käyttäjä avaa kohdesovelluksen kertakirjautumispalvelun avulla ja valitsee työroolin
3. Identifiointipalvelu (identiteetinhallinta) tarkastaa tunnistustietoja vasten käyttäjän identiteetin käyttövaltuushakemistosta. Käyttövaltuushakemistosta palautuvat tarvittavat identiteetti- ja valtuustiedot (tunnistusseloste).
4. Kertakirjautumisen sessio luodaan

5. Kertakirjautumispalvelu suorittaa tunnistautumisen kohdesovellukseen käyttäjän puolesta (usein syöttää käyttäjän käyttäjätunnuksen ja salasanan).
6. Kohdesovellus aukeaa käyttäjälle

Hyvät ja huonot puolet:

+ ei vaadi muutoksia kohdesovelluksiin
+ toimii useiden sovellusteknologioiden kanssa (Windows, Java, web, pääte-emulaattorit jne.)
+ mahdollistaa ns. kioski-moodin yhteiskäyttöisillä työasemilla
- Edellyttää kertakirjautumissovelluksen hankintaa ja käyttöönottoa

3.1.2 (Web) Kertakirjautuminen hakemistointegraation (esim paikallinen hakemisto) avulla



Kuva x: Kertakirjautuminen (myös Web) hakemistointegraation (esim.paikallinen hakemisto) avulla. Työntekijä kirjautuu sovellukseen

Esiehdot:

Työntekijän käyttövaltuudet ja identiteetti on provisioitu käyttövaltuuksien hallinnasta (luvitusprosessi) käyttäjä- ja käyttövaltuushakemistoon. Käyttövaltuuksien suhteen on tehty toinen seuraavista

- (a) identiteetti- ja käyttövaltuustiedot on provisioitu kohdesovellukseen.
- (b) käyttövaltuudet on provisioitu hakemistoon.

1. Käyttäjän työasematunnistautuminen tehdään käyttäjä- ja käyttöoikeushakemistoa vasten.
2. Käyttäjälle perustetaan istunto hakemistoon.
   - hakemisto pitää kirjaa, ketkä ovat kirjautuneet ja mitä oikeuksia heillä on
   - hakemistolta voidaan kysyä käyttäjän oikeuksia, tiketin voimassaoloa
3. Käyttäjä avaa kohdesovelluksen/ Web sovelluksen.
4. a. Työasema antaa käyttäjän identiteetin kohdesovellukselle. Kohdesovellus tarkastaa käyttäjän identiteetin hakemiston istuntoa vasten. Käyttövaltuudet sovellus

saa omasta kannastaan.
b. Työasema välittää käyttäjän identiteetin kohdesovellukselle, joka tarkastaa käyttäjän identiteetin hakemiston istuntoa vasten sekä hakee käyttövaltuudet hakemistosta.

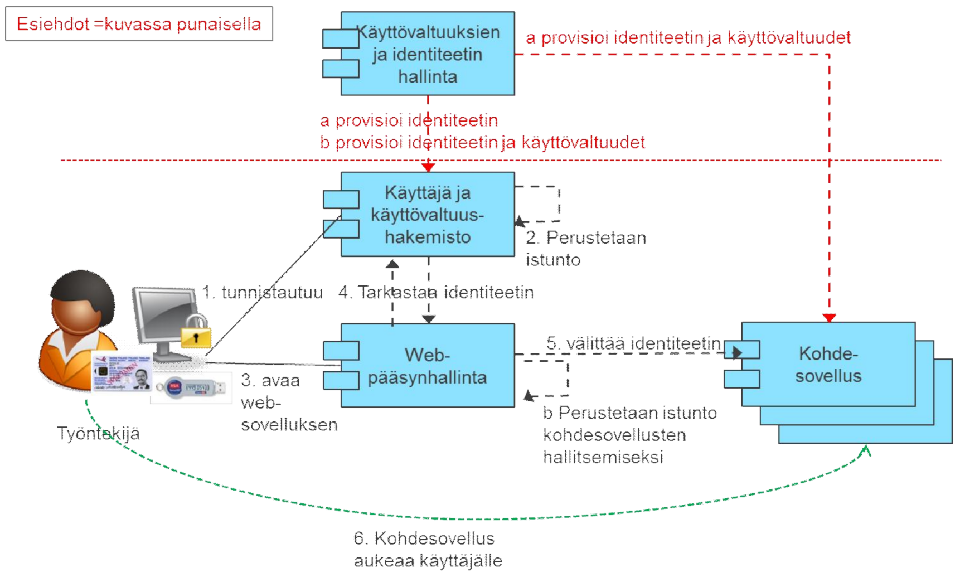
5. Kohdesovellus avautuu käyttäjälle.

Hyvät ja huonot puolet:
+ ei vaadi yleensä uusien tietojärjestelmäpalveluiden hankkimista
- kohdesovellus on integroitava käyttövaltuushakemistoon (sovelluksessa on oltava tämä ominaisuus valmiina tai se on rakennettava sovellukseen)
- hakemiston hallinta ja lähtötilanteen analysointi pitää hoitaa ulkoisella menettelyllä (tikettijärjestelmä, sähköposti) jolloin raportointi ja valvonta ei välttämättä järjestelmällistä tai tehokasta.

Kertakirjautuminen suoraan:
- toimii suppeamman sovellusteknologiajoukon kanssa (Windows verkko, web palvelut rajatusti -oman hakemiston ulottuvissa)
- kioski-moodi ei välttämättä toimi näin toteutetun kirjautumisen kanssa tai vaatii erillistä sovitustyötä (riippuu kioski-moodin toteutuksesta)

Web kertakirjautuminen:
- toimii vain käyttäjä- ja käyttövaltuushakemiston tunnistautumiseen nojaavissa päätelaitteissa
- toimintatapaa ei ole standardi ja tuki löytyy vain tietyissä selaimissa ja palvelinohjelmistoissa
- jokaiseen sovellukseen joudutaan rakentamaan kertakirjautuminen erikseen
- muut kirjautumistavat joudutaan rakentamaan jokaiseen sovellukseen erikseen

3.1.3 Kertakirjautuminen web-pääsynhallinnan avulla



Web pääsynhallinta:
1. Web pääsynhallinta pitää listaa kohdesovelluksista, session perustaminen ja purkaminen
2. Sisäänrakennettu pääsynhallinta, domainkohtaiset setup:t

Kuva x: Kertakirjautuminen web-pääsynhallinnan avulla. Kertakirjautuminen federoidussa pääsynhallinnassa

Esiehdot:
Käyttäjän käyttövaltuudet ja identiteetti on provisioitu käyttövaltuuksien hallinnasta (luvitusprosessi) käyttäjä- ja käyttövaltuushakemistoon. Käyttövaltuuksien suhteen on tehty toinen seuraavista

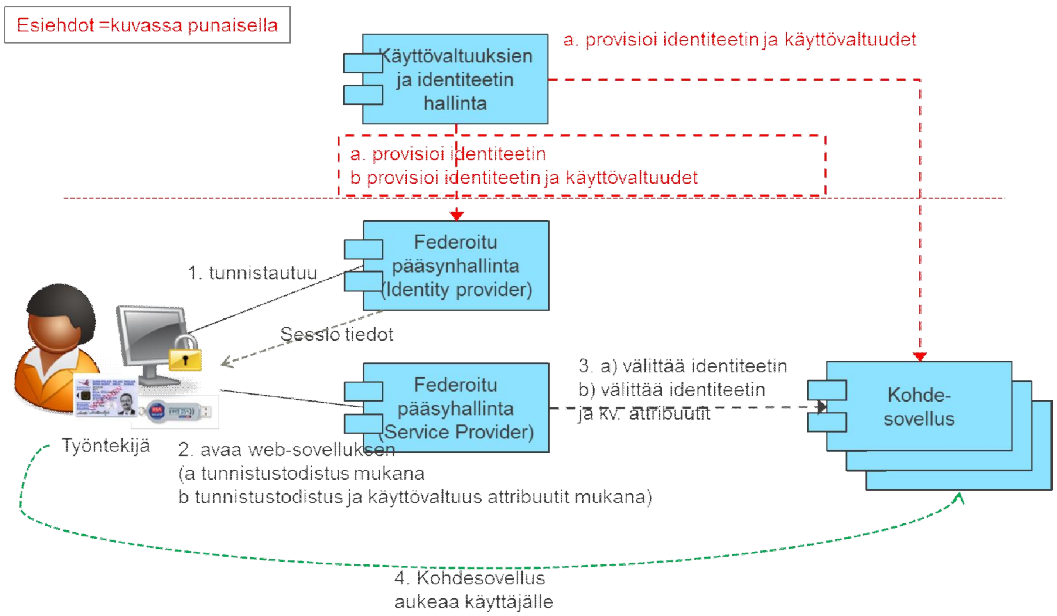
- (a) käyttäjä- ja käyttövaltuustiedot on provisioitu kohdesovellukseen.
- (b) käyttövaltuudet on provisioitu hakemistoon.

1. Käyttäjän työasematunnistautuminen tehdään käyttäjä- ja käyttöoikeushakemistoa vasten.
2. Käyttäjälle perustetaan istunto hakemistoon.
    - hakemisto pitää kirjaa, ketkä ovat kirjautuneet ja mitä oikeuksia heillä on
    - hakemistolta voidaan kysyä käyttäjän oikeuksia, tiketin voimassaoloa
3. Käyttäjä avaa web-sovelluksen.
4. Työasema välittää käyttäjän identiteetin web-pääsynhallinnalle, joka tarkastaa käyttäjän identiteetin hakemiston istuntoa vasten.
5. a) web-pääsynhallinta välittää käyttäjän tarkastetun identiteetin kohdesovellukselle. Kohdesovellus saa käyttövaltuudet omasta kannastaan.
   b) web-pääsynhallinta välittää käyttäjän tarkastetun identiteetin ja käyttövaltuudet kohdesovellukselle, luo sekä ylläpitää sessiota kohdesovellusten hallitsemiseksi. (Huom sessi pitää purkaa hallitusti hakemistosession purkamisen yhteydessä) Myös vaihtoehto c) on mahdollinen: web-pääsynhallinta voi toimia myös pelkän identiteetin tarkastajan roolissa, jolloin kohdesovellus hakee käyttäjän käyttövaltuudet hakemistosta

6. Kohdesovellus avautuu käyttäjälle.

Hyvät ja huonot puolet:
+ ei vaadi federointi - tietojärjestelmäpalveluiden hankkimista
+ web-pääsynhallinta pystyy tarjoamaan kertakirjautumisen myös muille tunnistustavoille (esim. kt+ss)
+ voidaan tallentaa muiden web-palveluiden käyttäjätunnuksia ja salasanoja varastoon (toimii kuten ESSO, mutta vain web-ympäristössä; kaikki WAM tuotteet eivät tue tätä toimintatapaa)
- web-pääsynhallinta on integroitava käyttövaltuushakemistoon (tuotteen on tuettava tätä ominaisuutta)
- toimii vain käyttäjä- ja käyttövaltuushakemiston tunnistautumiseen nojaavissa päätelaitteissa
- toimintatapaa ei ole standardi ja tuki löytyy vain tietyissä selaimissa ja palvelinohjelmistoissa
- Jokaiseen sovellukseen joudutaan rakentamaan kertakirjautuminen erikseen

3.1.4 Kertakirjautuminen federoidussa pääsynhallinnassa



Kuva x: Kertakirjautuminen federoidussa pääsynhallinnassa, jossa -a) identiteetit ja käyttövaltuudet provisioidaan erikseen tai b) käyttövaltuudet välitetään attribuutteina

Esiehdot:

- a) Käyttäjän identiteetti on provisioitu Identity providerille. Käyttövaltuudet ja identiteetti on provisioitu kohdesovellukseen.
- b) Käyttäjän identiteetti ja käyttövaltuudet on provisioitu Identity Providerille

1. Käyttäjän tunnistautuu Federoidun käyttäjähallinnan Identity Provideriin. Käyttäjälle perustetaan istunto federoinnin lähdehakemistoon. Federoinnin kohdehakemistoon perustetaan vastaava istunto, johon tuodaan tiedot lähdehakemistosta.
2. a) Käyttäjä avaa web-sovelluksen. Mukana siirtyy Identity Provideriltä saatu todistus identiteetin tunnistuksesta (tunnistusseloste eli ” tiketti”).

   b) Käyttäjä avaa web-sovelluksen. Mukana siirtyy Identity Provideriltä saatu todistus identiteetin tunnistuksesta sekä käyttövaltuudet sisältävät attribuutit
3. a) Federoidun pääsynhallinnan Service Provider tarkastaa todistuksen aitouden ja sen että Identity Provider kuuluu luotettuihin tunnistajiin. Federoitu pääsynhallinta välittää käyttäjän identiteetin kohdesovellukselle.
   Kohdesovellus saa käyttövaltuudet omasta kannastaan, istunto perustetaan.

   b) Federoidun pääsynhallinnan Service Provider tarkastaa todistuksen aitouden ja sen että Identity Provider kuuluu luotettuihin tunnistajiin. Federoitu pääsynhallinta välittää käyttäjän identiteetin sekä käyttövaltuudet sisältävät attribuutit kohdesovellukselle.
   Kohdesovellus saa käyttövaltuudet attribuuttien arvoista, istunto perustetaan
4. Kohdesovellus avautuu käyttäjälle.

Muita vaihtoehtoja:
Vaihtoehto, kohta:1 Työntekijä yrittää avata suoraan web-sovellusta

- Federoidun pääsyhallinnan Service Provider tietojärjestelmäpalvelu tarkastaa, onko käyttäjällä voimassa oleva istunto.
- Jos käyttäjällä on voimassa oleva istunto, hänen ei tarvitse tunnistautua uudestaan.
- Jos voimassa olevaa istuntoa ei ole, käyttäjä ohjataan tunnistautumaan Identity Providerille.

Vaihtoehto b) käyttövaltuudet välitetään attribuutteina

Kohdesovellus voi myös perustaa käyttäjälle identiteetin ja käyttövaltuustiedot omaan käyttäjäkantaansa. Ongelmana tässä toimintatavassa on se, että kohdesovelluksen yläpuolella oleva identiteetinhallinta ei tiedä tällä tavalla perustettuja käyttäjiä.

Hyvät ja huonot puolet:
+ standardoidut tavat toteuttaa federointi
+ useimmat yleisesti käytetyt selaimet, päätelaitteet ja käyttöjärjestelmät tukevat toimintatapaa
+ pystyy tarjoamaan kertakirjautumisen luottamusverkoston sisällä
- käyttäjät ja käyttövaltuudet pitää toimittaa erikseen kohdesovellukselle (jos omassa organisaatiossa) tai mahdollisesti toisen organisaation identiteetinhallinnalle (jos kohdesovellus toisessa organisaatiossa)
- vaatii federointiteknologian käyttöönoton kummassakin päässä
- luottamusverkosto pitää konfiguroida etukäteen
<u>a) identiteetit ja käyttövaltuudet provisioidaan erikseen</u>

- + kohdesovelluksen käyttäjät ovat ennalta tiedossa

b) käyttövaltuudet välitetään attribuutteina

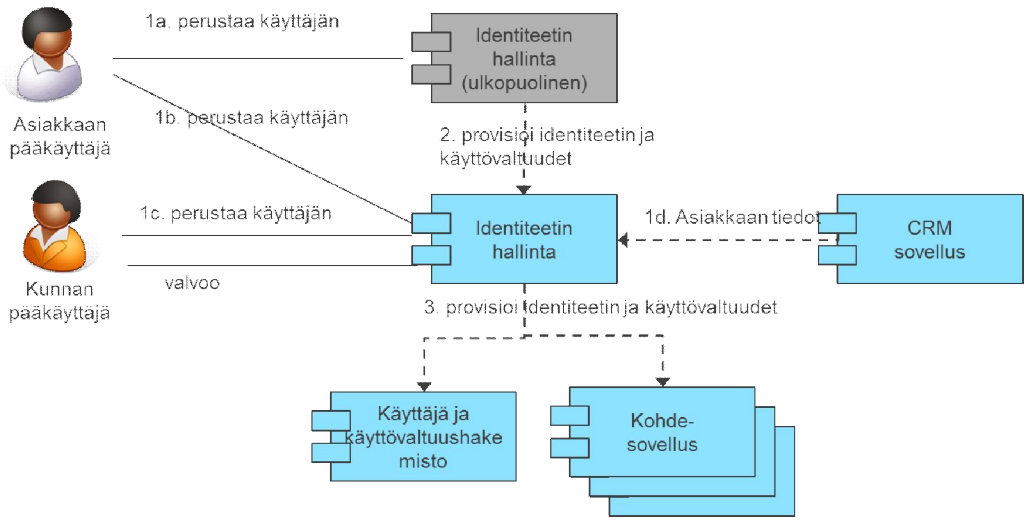
- + kohdesovelluksen käyttäjien ei tarvitse olla etukäteen kohdesovelluksen tiedossa. Tieto saattaa löytyä vain käyttölokeilta
- - Idenity providerin pitää olla ketterä, uusia attribuutteja saatetaan joutua lisäämään uusien kohdesovellusten myötä

3.2 Käyttövaltuuksien ja identiteetin hallinta ja valvonta- Asiakaskäyttäjät

Erilaiset tunnistautumis- ja valtuutuskäytönnöt johtavat myös erilaisiin ylläpitokäytäntöihin. Erilaisille asiakaita koskeville kertakirjautumistavoille on tässä esitetty seuraavat hallinta- ja valvontatavat (kunnan työntekijät hallitaan prosessien mukaisesti):

- **Kertakirjautuminen web-pääsynhallinnan avulla (ks. Asiakaskäyttäjät)**
  - Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (ilman federointia)
  - Henkilöasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (ilman federointia)
- **Web-kertakirjautuminen federoidussa tunnistuksessa (identiteettien ja käyttövaltuuksien provisiointi erikseen) (ks. Asiakaskäyttäjät)**
  - Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (federoitu identiteetti ja käyttövaltuudet provisioidaan)
- **Web-kertakirjautuminen federoidussa tunnistuksessa (käyttövaltuudet attribuutteina) (ks. Asiakaskäyttäjät)**
  - Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (pelkkä federointi)
  - Henkilöasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (pelkkä federointi)
  - Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (ilman federointia)

3.2.1 Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (ilman federointia)



Kuva x: Organisaatioasiakkaiden käyttövaltuuksien luonti ja provisiointi ilman federointia. Kertakirjautuminen hallitaan Web-pääsynhallinnan avulla (ks. asiakaskäyttäjät - kertakirjautuminen)

a) Asiakaskäyttäjät perustetaan kotiorganisaatiossaan:

1. Asiakkaan pääkäyttäjä perustaa organisaation käyttäjän ja antaa hänelle käyttövaltuudet oman organisaationsa identiteetinhallintajärjestelmässä.
2. Asiakasorganisaation identiteetinhallinta provisioi käyttäjän identiteetti- ja käyttövaltuustiedot kunnan käyttämään käyttövaltuus ja identiteetinhallintajärjestelmään
3. Kunnan käyttövaltuushallinta provisioi identiteetin ja käyttövaltuudet hakemistoihin ja kohdesovelluksiin.

b) asiakaskäyttäjät perustetaan kunnan käyttövaltuus ja identiteetin hallintajärjestelmään

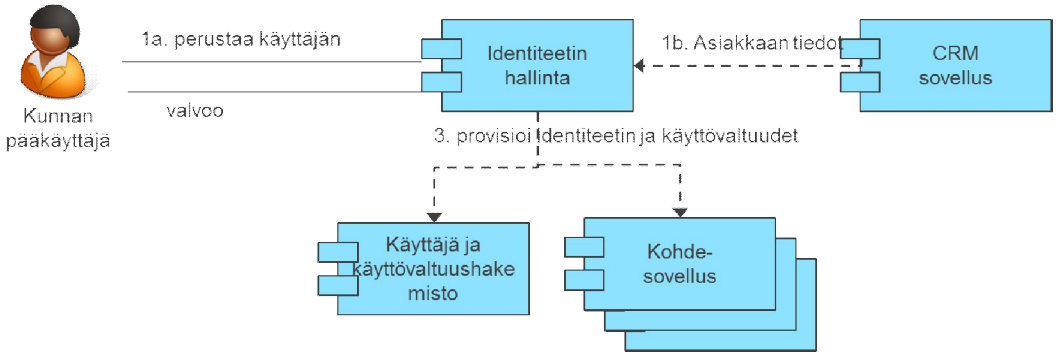
1. a) Asiakkaan pääkäyttäjä perustaa (organisaation) käyttäjän ja käyttövaltuudet kunnan käyttämään identiteetinhallintajärjestelmään.
   b) Kunnan pääkäyttäjä perustaa asiakaskäyttäjän ja käyttövaltuudet kunnan käyttämään identiteetinhallintaan.
2. -
3. Kunnan identiteetinhallinta provisioi identiteetin ja käyttövaltuudet hakemistoihin ja kohdesovelluksiin.

Muut vaihtoehdot menevät samalla tavalla kuin vaihtoehto (b), mutta niissä asiakastiedot ja käyttövaltuudet perustetaan seuraavilla eri mekanismeillä:

- (1d) CRM-sovellus toimittaa asiakkaan identiteetin ja käyttövaltuustiedot kunnan käyttämään identiteetinhallintaan.
- CRM-sovelluksen sijaan tiedot voivat tulla myös ydintiedon hallinnasta (MDM).

Kun käyttäjän identiteetti- ja käyttövaltuustiedot perustetaan tai välitetään kunnan identiteetinhallinnan kautta, voi kunnan pääkäyttäjä myös valvoa niitä (kenellä käyttäjällä on millaiset oikeudet).

3.2.2 Henkilöasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (ilman federointia)



Kuva x: Henkilöasiakkaiden käyttövaltuuksien luonti ja provisiointi ilman federointia. Kertakirjautuminen hallitaan Web-pääsynhallinnan avulla (ks. asiakaskäyttäjät - kerta-kirjautuminen)

Henkilöasiakkaat perustetaan ja aktivoidaan käyttäjiksi

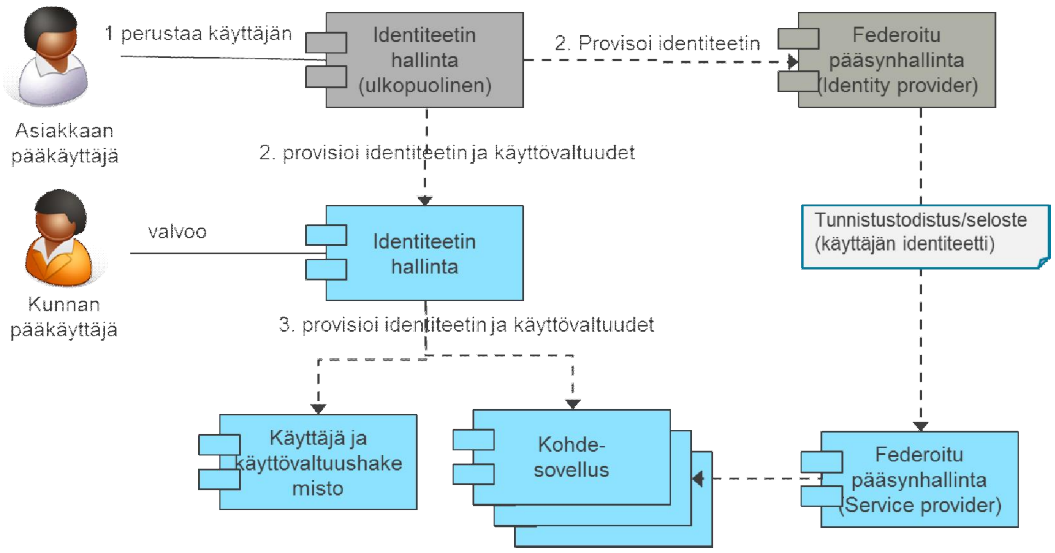
a) Kunnan pääkäyttäjä perustaa henkilöasiakaskäyttäjän ja antaa hänelle käyttövaltuudet kunnan käyttämässä identiteetinhallintajärjestelmässä

b) CRM-sovellus toimittaa asiakkaan identiteetin ja käyttövaltuustiedot kunnan käyttämään identiteetinhallintaan.

Kunnan identiteetinhallinta provisioi identiteetin ja käyttövaltuudet hakemistoihin ja kohdesovelluksiin.

Kun käyttäjän identiteetti- ja käyttövaltuustiedot perustetaan tai välitetään kunnan identiteetinhallinnan kautta, voi kunnan pääkäyttäjä myös valvoa niitä (kenellä käyttäjällä on millaiset oikeudet).

3.2.3 Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (identiteetti ja käyttövaltuudet provisioidaan)



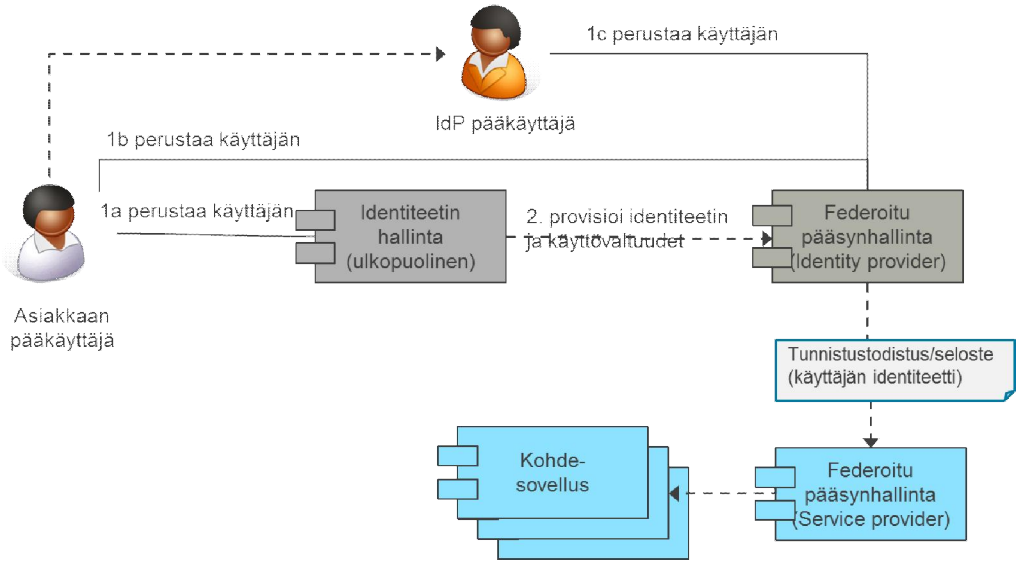
Kuva x: Organisaatioasiakkaiden käyttövaltuuksien luonti ja provisiointi federoidussa pääsynhallinnassa. Kertakirjautuminen hallitaan federoidun tunnistuksen mukaisesti (ks. asiakaskäyttäjät - kertakirjautuminen)

Tapahtumien kulku:

1. Asiakkaan pääkäyttäjä perustaa organisaation käyttäjän ja antaa hänelle käyttövaltuudet oman organisaationsa identiteetinhallintajärjestelmässä.
2. Asiakasorganisaation identiteetinhallinta provisioi käyttäjän identiteetti- ja käyttövaltuustiedot kunnan käyttämään identiteetinhallintajärjestelmään sekä asiakkaan käyttämälle Identity providerille.
3. Kunnan identiteetinhallinta provisioi identiteetin ja käyttövaltuudet hakemistoihin ja kohdesovelluksiin.

Kun käyttäjän identiteetti- ja käyttövaltuustiedot välitetään kunnan identiteetinhallinnan kautta, voi kunnan pääkäyttäjä myös valvoa niitä (kenellä käyttäjällä on millaiset oikeudet).

3.2.4 Organisaatioasiakkaiden identiteetin ja käyttöoikeuksien hallinta ja valvonta (pelkkä federointi)



Kuva x: Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta- pelkkä federointi. Kertakirjautumisen hallinta: Web-kertakirjautuminen federoidussa tunnistuksessa -käyttövaltuudet attribuutteina (ks. asiakaskäyttäjät – kertakirjautuminen)

Käyttäjä perustetaan kotiorganisaationsa identiteetinhallintaan

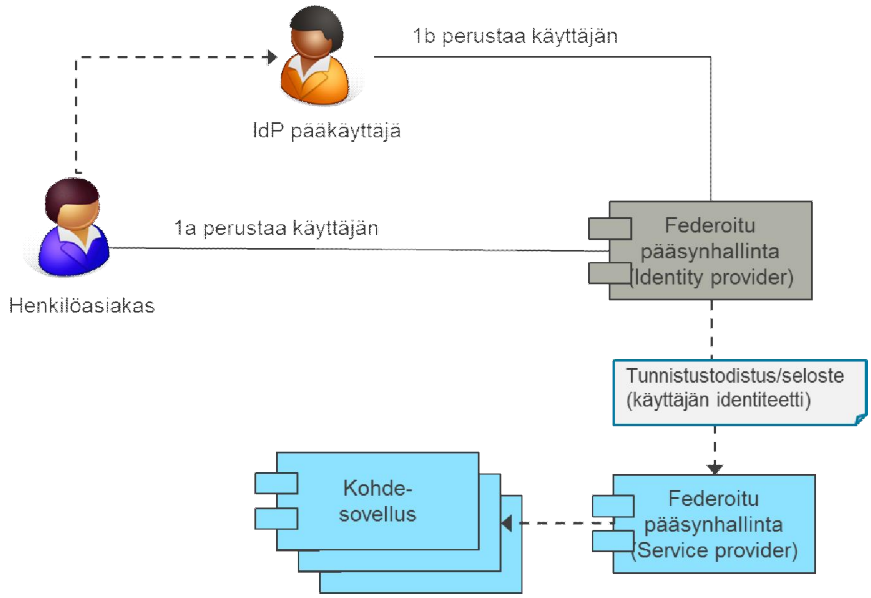
1. Asiakkaan pääkäyttäjä perustaa organisaation käyttäjän ja antaa hänelle käyttövaltuudet oman organisaationsa identiteetinhallintajärjestelmässä (a)
2. Asiakasorganisaation identiteetinhallinta provisioi käyttäjän identiteetti- ja käyttövaltuustiedot asiakkaan käyttämälle Identity providerille. Identiteetti ja käyttövaltuudet välittyvät tunnistustodistuksen mukana Idenitty providerilta kunnan Service providerille.

Muut mahdolliset tavat käyttäjän ja käyttövaltuuksien perustamiseksi:

1. Asiakkaan pääkäyttäjä perustaa organisaation käyttäjän ja antaa hänelle käyttövaltuudet suoraan Identity provideriin (b)
2. Asiakkaan pääkäyttäjä pyytää Identity providerin pääkäyttäjää perustamaan käyttäjän ja käyttöoikeudet (c)

Kun identiteetti- ja käyttövaltuustiedot eivät välity kunnan identiteetinhallinnan kautta, niitä voidaan seurata vain jälkikäteen lokeilta. Etukäteen ei voida tietää, keille kukin asiakasorganisaatio on antanut millaisiakin käyttöoikeuksia. Näissä tapauksissa tuleekin sopimuksellisesti siirtää kaikki käyttäjäidentiteetteihin ja käyttövaltuuksiin liittyvät ongelmatilanteet siirtää asiakkaan vastuulle, sillä kunnan on hyvin hankalaa tai mahdotonta tietää ja vaikuttaa käyttäjiin ja käyttövaltuuksiin.

3.2.5 Henkilöasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (pelkkä federointi)



Kuva x: Henkilöasiakkaiden identiteetin ja käyttövaltuuksien hallinta- pelkkä federointi. Kertakirjautumisen hallinta: Web-kertakirjautuminen federoidussa tunnistuksessa käyttövaltuudet attribuutteina (ks. asiakaskäyttäjät - kertakirjautuminen)

Itsepalvelu:

- a) Henkilöasiakas perustaa itse itsensä Identity provideriin (ja antaa tarvittava oikeudet). Identiteetti- ja käyttövaltuudet välittyvät tunnistustodistuksen mukana Idenitty providerilta kunnan Service providerille.

Delegointi

- (b) Henkilöasiakas pyytää Identity providerin pääkäyttäjää perustamaan hänelle identiteetin ja käyttövaltuudet.

Kun identiteetti- ja käyttövaltuustiedot eivät välity kunnan identiteetinhallinnan kautta, niitä voidaan seurata vain jälkikäteen lokeilta. Etukäteen ei voida tietää, ketkä ovat mahdollisia käyttäjiä (ja millaisia käyttövaltuuksia heillä on). Näissä tapauksissa tuleekin sopimuksellisesti siirtää kaikki käyttäjäidentiteetteihin ja käyttövaltuuksiin liittyvät ongelmatilanteet asiakkaan vastuulle, sillä kunnan on hyvin hankalaa tai mahdotonta tietää ja vaikuttaa käyttäjiin ja käyttövaltuuksiin.

Huom. Perustaminen voi olla myös ”puoliautomaattista/välillistä”. Esim. VETUMA-tunnistus (Identity provider) nojaa pankkien TUPAS-tunnistukseen, jonka käyttäjätunnus luodaan nettipankin käyttöönoton yhteydessä.

3.3 Asiakaskäyttäjät

Asiakaskäyttäjille käytetty käyttövaltuuksien ja identiteetinhallintajärjestelmä ei tarvitse olla sama kuin työntekijöille, sillä asiakaskäyttäjien kohdalla esimerkiksi hyväksyn-

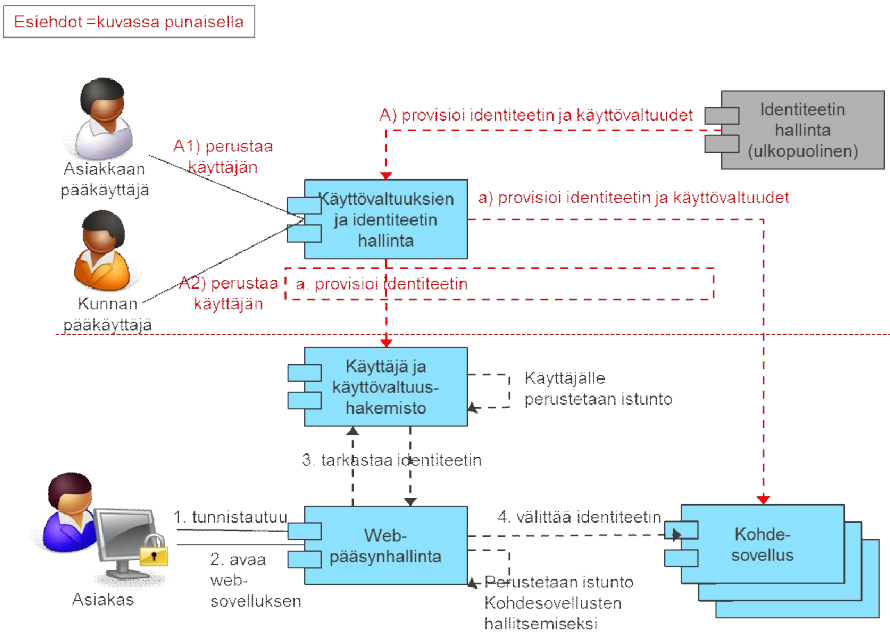
töihin liittyvälle kierrätykselle ei ole yleensä tarvetta. Asiakaskäyttöliittymät toimivat joskus teknisten tunnusten varassa, jolloin heitä ei välttämättä identifioida tai perusteta samalla tavalla käyttäjiksi kuin kunnan työntekijöitä, joten provisioinnit ovat erilaisia. Teknisten tunnusten käyttämisestä tulee pyrkiä eroon tavoitetilassa ja kaikkia käyttäjäryhmiä tulisi kohdella samalla tavalla.

Asiakaskäyttäjä kertakirjautuu sovellukseen
Toistaiseksi tällaiselle tyyppitapaukselle ei ole tunnistettu tarvetta, vaan asiakaskäyttäjät käyttävät aina web-sovelluksia/käyttöliittymiä.

Asiakaskäyttäjä kertakirjautuu web-sovellukseen
Asiakaskäyttäjien kohdalla ratkaisuvaihtoehdot ovat periaatteessa samat kuin kunnan työntekijöiden kohdalla lukuun ottamatta hakemistointegraatioon perustuvaa toimintamallia, joka ei ole käytännön realiteetit huomioon ottaen mahdollinen.
Mahdollisia ratkaisuehdokkaita ovat siis aiempana esitetyt (pienin muutoksin):

- Kertakirjautuminen web-pääsynhallinnan avulla
- web-kertakirjautuminen federoidussa tunnistuksessa
    - **a**) identiteettien ja käyttövaltuuksien provisiointi erikseen
    - **b**) käyttövaltuudet attribuutteina

3.3.1 Kertakirjautuminen web-pääsynhallinnan avulla



Kuva x: Kertakirjautuminen web-pääsynhallinnan avulla. Asiakas kirjautuu sovellukseen Web:n kautta
Esiehdot:

- (A) Asiakkaan käyttämä ulkoinen identiteetin hallinta provisioi identiteetin käyttövaltuuksien ja identiteetin hallintaan.

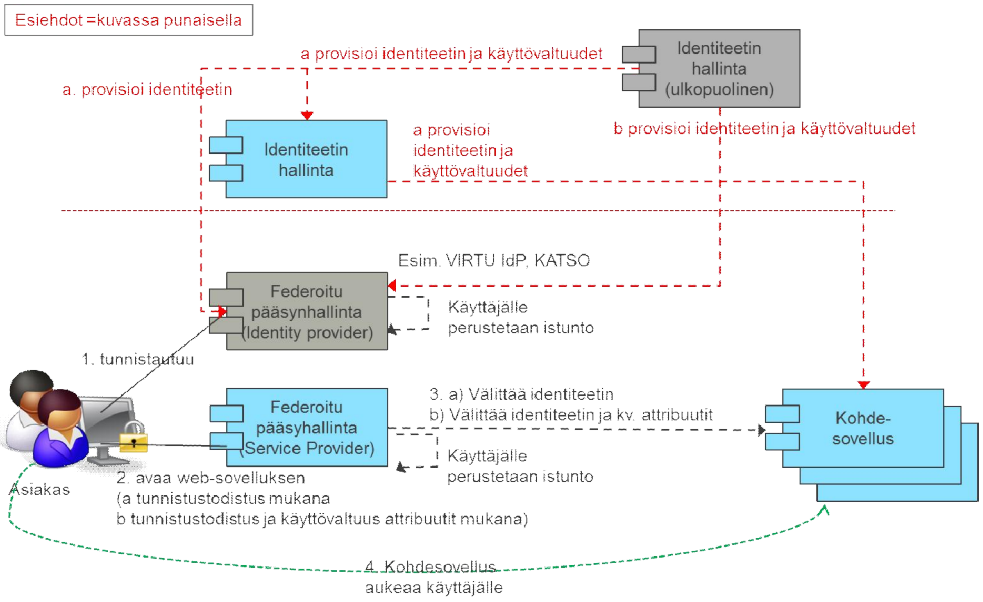
- A1 Asiakkaan pääkäyttäjä ylläpitää niitä suoraan kunnan käyttämään identiteetin hallintaan
- A2. Kunnan pääkäyttäjä ylläpitää niitä suoraan kunnan käyttämään identiteetin hallintaan

- Käyttäjän käyttövaltuudet ja identiteetti on provisioitu käyttövaltuuksien hallinnasta (luvitusprosessi) käyttäjä- ja käyttövaltuushakemistoon ja lisäksi
  - (a) käyttäjä- ja käyttövaltuustiedot on provisioitu kohdesovellukseen.

1. Asiakas tunnistautuu web pääsynhallintaan ja tunnistaminen tehdään käyttäjä- ja käyttöoikeushakemistoa vasten. Käyttäjälle perustetaan istunto käyttövaltuushakemistoon.
2. Asiakas avaa web-sovelluksen.
3. Työasema välittää käyttäjän identiteetin web-pääsynhallinnalle, joka tarkastaa käyttäjän identiteetin hakemiston istuntoa vasten.
4. web-pääsynhallinta välittää käyttäjän tarkastetun identiteetin kohdesovellukselle. Kohdesovellus saa käyttövaltuudet omasta kannastaan, luo session kohdesovellusten hallitsemiseksi.
5. Kohdesovellus avautuu käyttäjälle.

Asiakas on aktivoitu ja valtuudet luotu kohtien 3.2.1 Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (ilman federointia) ja
ja 3.2.2 Henkilöasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (ilman federointia) mukaisesti

3.3.2 Web-kertakirjautuminen federoidussa tunnistuksessa



Kuva x: Kertakirjautuminen federoidussa pääsynhallinnassa, jossa -a) identiteetit ja käyttövaltuudet provisioidaan erikseen tai b) käyttövaltuudet välitetään attribuutteina

Esiehdot:

a) Identiteetti ja käyttövaltuustiedot on välitetty asiakkaan käyttämästä identiteetin hallinnasta kunnan käyttämään identiteetinhallintaa.
Identiteetti on provisioitu federoidun pääsynhallinnan identity provideriin (joka on usein eri kuin kunnan käyttämä).
Käyttövaltuudet ja identiteetti on provisioitu kohdesovellukseen.
b) Käyttäjän identiteetti ja käyttövaltuudet on provisioitu Identity Providerille.
Käyttövaltuudet välitetään kohdesovelluksille.

1. Käyttäjän tunnistautuu Federoidun käyttäjähallinnan Identity Provideriin. Käyttäjälle perustetaan istunto identity provideriin ja service provideriin.
2. a) Käyttäjä avaa web-sovelluksen. Mukana siirtyy Identity Provideriltä saatu todistus identiteetin tunnistuksesta (tunnistustodistus eli ” tiketti”).

   b) Käyttäjä avaa web-sovelluksen. Mukana siirtyy Identity Provideriltä saatu todistus identiteetin tunnistuksesta sekä käyttövaltuudet sisältävät attribuutit
3. a) Federoidun pääsynhallinnan Service Provider tarkastaa todistuksen aitouden ja sen että Identity Provider kuuluu luotettuihin tunnistajiin. Federoitu pääsynhallinta välittää käyttäjän identiteetin kohdesovellukselle.
   Kohdesovellus saa käyttövaltuudet omasta kannastaan.

   b) Federoidun pääsynhallinnan Service Provider tarkastaa todistuksen aitouden ja sen että Identity Provider kuuluu luotettuihin tunnistajiin. Federoitu pääsynhallinta välittää käyttäjän identiteetin sekä käyttövaltuudet sisältävät attribuutit kohdesovellukselle.
   Kohdesovellus saa käyttövaltuudet attribuuttien arvoista.
4. Kohdesovellus avautuu käyttäjälle.

HUOM. Erona lähinnä se työntekijän kertakirjautumiseen federoidussa tunnistuksessa:

a) identiteetti- ja käyttövaltuustiedot välitetään asiakkaan käyttämästä identiteetinhallinnasta kunnan käyttämään identiteetinhallintaan. Identiteetti provisioidaan federoidun pääsynhallinnan identity provideriin, joka on usein eri kuin kunnan käyttämä.
b)identiteetti- ja käyttövaltuustiedot välitetään asiakkaan käyttämästä identiteetinhallinnasta federoidun pääsynhallinnan identity provideriin, joka on usein eri kuin kunnan käyttämä. Huom! Käyttäjän identiteetti voi olla identity providerin käytössä ilman provisiointia tai perustamista. (esim. VETUMA hyödyntää pankkien TUPAS-tunnistusta, joten käyttäjää ei tarvitse erikseen perustaa VETUMA:an).

Asiakas on aktivoitu ja valtuudet luotu kohtien 3.2.3 Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (identiteetti ja käyttövaltuudet provisioidaan) vaihtoehdolle a, 3.2.4 Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (pelkkä federointi) ja 3.2.5 Henkilöasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (pelkkä federointi) vaihtoehdolle b mukaisesti

Hyvät ja huonot puolet:

+ Käyttäjien hallinta vastuutettu selkeästi kumppaneille
+ mahdollistaa kertakirjautumiskokemuksen kumppanin verkosta
+ Käyttöoikeus voidaan purkaa heti myös kumppanin taholta
+ saadaan ajantasainen tieto kumppanin käyttäjien tilasta (ryhmät, attribuutit jne)
- verkoston hajauttaminen lisää valvottavien ja auditoitavien kohteiden määrää
- Kumppanin alihankintaketju tai muut kumppanin IDP:n luvittamat käyttäjät voivat muodostaa ennakoimattomia tilanteita mikäli sopimusrakenteet ja/tai prosessit eivät ole kunnossa kumppanin kanssa.

3.4 Kumppanityöntekijä omassa verkossa

Kumppanien työntekijöille tarjottavat etäyhteydet kunnan sovelluksiin - muut kuin web-sovellukset - toteutetaan pääasiassa virtualisoitujen työasema-asiakasohjelmien kautta (esim. Citrix client). Tällöin kumppanien käyttäjille annetaan AD-käyttäjätunnus, jolla he kirjautuvat kunnan käyttöoikeusverkkoon. Näin olleen vaikka kumppanin työntekijä istuukin omalla toimistollaan, hän on kirjautunut kunnan käyttö oikeusverkkoon. Tämän takia tämä tapaus on sama kuin 3.1 Kunnan työntekijät ja kumppanit kunnan verkossa eikä kuulu tämän otsikon alle (Kumppanin työntekijä omassa verkossa).

3.4.1 Kumppanikäyttäjä kertakirjautuu web-sovellukseen

Omassa käyttöoikeusverkossaan toimivien kumppanikäyttäjien web-kertakirjautumiseen liittyvät toimintamallit ovat samat kuin organisaatioasiakkailla luvussa 3.3 Asiakaskäyttäjät eli

- Kertakirjautuminen web-pääsynhallinnan avulla
- web-kertakirjautuminen federoidussa tunnistuksessa (identiteettien ja käyttövaltuuksien provisiointi erikseen)
- web-kertakirjautuminen federoidussa tunnistuksessa (käyttövaltuudet attribuutteina)

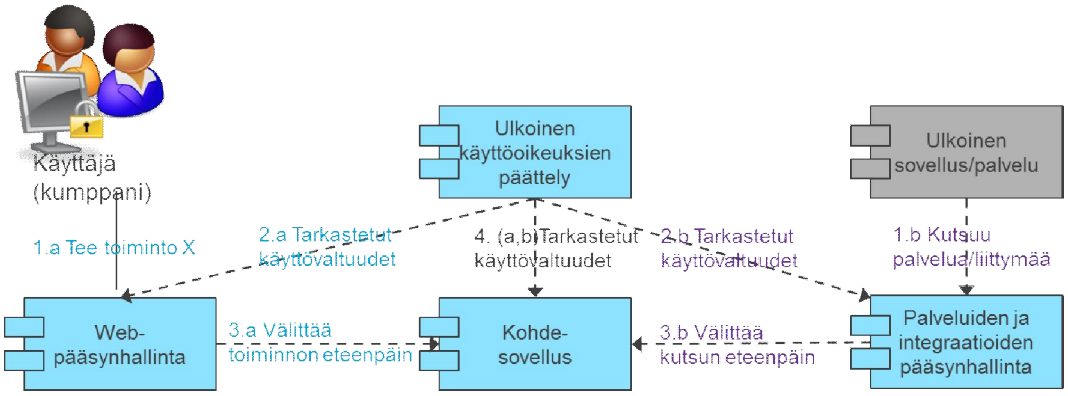
3.4.2 Kumppanikäyttäjän identiteetin ja käyttövaltuuksien hallinta ja valvonta

Omassa käyttöoikeusverkossaan toimivien kumppanikäyttäjien hallintaan ja valvontaan liittyvät toimintamallit ovat samat kuin organisaatioasiakkailla luvussa 3.2 Käyttövaltuuksien ja identiteetin hallinta ja valvonta- Asiakaskäyttäjät eli

- Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (ilman federointia)
- Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (identiteetti ja käyttövaltuudet provisioidaan)
- Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (pelkkä federointi)

3.5 Muita toimintamalleja

3.5.1 Ulkoinen käyttöoikeuksien päättely (EXT)



Kuva x: Ulkoinen käyttöoikeuksien päättely

Tapahtumien kulku (a) eli käyttäjä käyttää web-sovellusta

- Käyttäjä tekee toiminnon X
- web-pääsynhallinta tarkastuttaa ulkoisella käyttöoikeuksien päättelyllä käyttövaltuudet - karkea käyttövaltuuksien tarkastus (coarse grained), esimerkiksi tunnistetaan lähde, josta käyttäjä saapuu
- web-pääsynhallinta välittää toiminnon eteenpäin kohdesovellukselle.
- Kohdesovellus tarkastuttaa ulkoisella käyttöoikeuksien päättelyllä käyttäjän hienojakoiset käyttöoikeudet (fine grained), tunnistetaan ulkoisen päättelyn vlitäämien tietojen avulla käyttäjän oikeutus kohdejärjestelmään ja sen sisäisiin ryhmiin.

Toinen vaihtoehto (b) eli ulkoinen sovellus/palvelu kutsuu kohdesovelluksen tarjoamaa palvelua tai integraatiota

- Ulkoinen sovellus/palvelu kutsuu kohdesovelluksen tarjoamaa palvelua tai liittymää
- Palveluiden ja integraatioiden pääsynhallinta tarkastuttaa ulkoisella käyttöoikeuksien päättelyllä käyttövaltuudet - karkea käyttövaltuuksien tarkastus (coarse grained)
- Palveluiden ja integraatioiden pääsynhallinta välittää kutsun eteenpäin kohdesovellukselle.
- Kohdesovellus tarkastuttaa ulkoisella käyttöoikeuksien päättelyllä hienojakoiset käyttöoikeudet (fine grained)

Karkean tason (kohta 2.) tai hienonjakoisen tason (kohta 4): käyttövaltuuksien tarkastukset voidaan tehdä joko kummatkin tai vain toinen tai ei kumpikaan ulkoisen käyttöoikeuksien päättelyn tietojärjestelmäpalvelun avulla.

Esimerkki ulkoisesta päättelystä on palveluntuottaja, joka hankkii kolmannelta osapuolelta tunnistuspalvelun, jota vasten liitetään tuottajan asiakkaat. Kunta asiakkaana kirjautuu palveluntuottajan järjestelmään, jossa tunnistetaan oikeutus kohdesovelluksen käyttöön ja mahdolliset kohdesovelluksen oikeutustasot ja attribuutit. Tämän jälkeen sessio siirretään tunnistetietoineen palveluntuottajan kohdesovellukselle.

Ulkoinen käyttöoikeuksien päättelylle lähetetään usein mm. seuraavat tiedot käyttäjä, toiminto joka aiotaan tehdä tai objekti, jonka tietoja haetaan/muutetaan/jne. Ulkoinen käyttöoikeuksien päättely vastaa, onko käyttäjällä oikeudet kyseiseen toimintoon.

Liite 2

Kuntasektorin arkkitehtuuriryhmä

Kuntasektorin käyttövaltuushallinnan viitearkkitehtuuri

Versio 1.0

Tiedonsiirron periaatteet ja aikakaaviot

Helsinki 2013

Kuntaliitto
Kommunförbundet

Sisältö

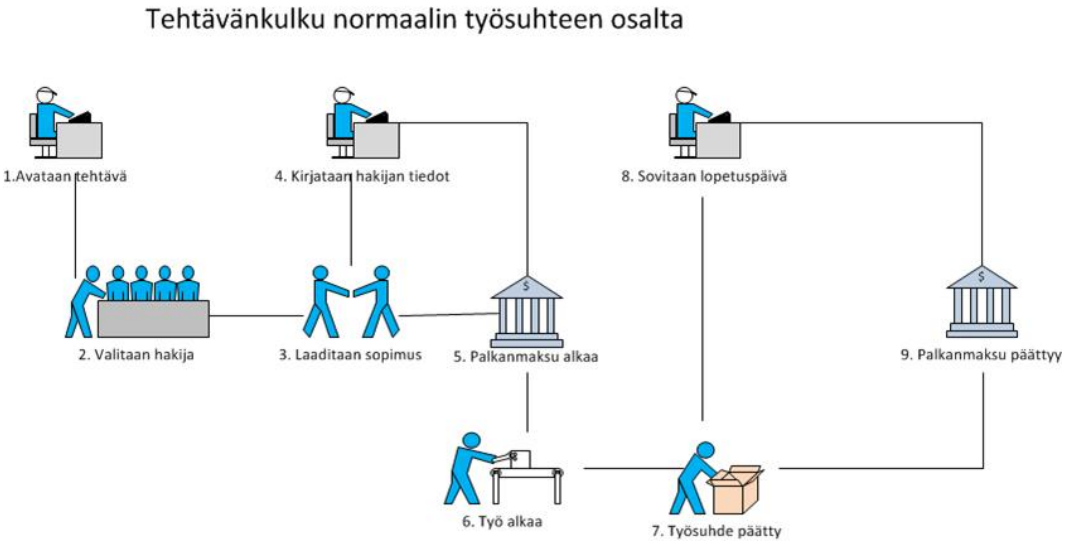
Johdanto

Tämä kuvaus on tarkoitettu käytettäväksi esimerkinomaisena ohjeena mietittäessä henkilön työsuhteen alkamista tai työsuhteen päättymistä käyttövaltuushallinnan näkökulmasta
Esimerkkien avulla voidaan hahmottaa ongelmakohdat, jotka liittyvät käyttövaltuuksien luonnin ja poistamisen ajoitukseen ja niiden esimerkkiratkaisuun. Kunnan tulee omien henkilöstöhallinnon järjestelmien puitteissa ratkaista miten käyttövaltuushallinnan ja henkilöstöhallinnon prosessit ja järjestelmät kommunikoivat, jotta ongelmat saadaan ratkaistua.

2 Henkilön palkkaus ja työsuhteen päättäminen

2.1 Tehtävänkulku normaalin työsuhteen osalta

Esimerkkiskenaariokuvauksessa käsitellään normaalia uuden henkilönpalkkausta ja työsuhteen alkamista käyttövaltuushallinnan näkökulmasta. Normaali työsuhde on joko vakituinen toistaiseksi voimassa oleva työsuhde tai pitkä määräaikaisuus, joka päättyy ennalta sovitusti.



Kuva 1 Henkilön työsuhteen alkaminen ja päättyminen

Normaalin työsuhteen sanallinen käyttökertomus:
Normaali työsuhde on joko vakituinen toistaiseksi voimassa oleva työsuhde tai pitkä määräaikaisuus, joka päättyy ennalta sovitusti.

1. Tehtävä avataan rekrytointia varten, jolloin määritellään mihin tehtävään/työrooliin ollaan hakemassa työntekijää. Henkilön tuleva esimies tai muu valtuutettu täyttää tehtävän kuvauksen.
2. Rekrytointiprosessin mukaisesti haetaan ja valitaan hakija työtehtävään/työrooliin. Henkilölle luodaan yksilöivä tunniste.

3. Esimies laatii työntekijän kanssa sopimuksen, jossa sovitaan aloittamispäivä. Esimies varmistaa myös hakijan identiteetin viimeistään sopimusta kirjoitettaessa. Tietoturvasitoumus tehdään tarvittaessa sopimuksen allekirjoituksen yhteydessä. Työntekijä allekirjoituksellaan hyväksyy tietoturvasitoumuksen.
4. Esimies kirjaa uuden henkilön perushenkilötiedot (liittää henkilön työrooliin) henkilöstöhallinnon web -tallennusjärjestelmään, kun tieto henkilön palkkauksesta on varmistunut eli kun sopimus on allekirjoitettu. Vaihtoehtoisesti, henkilön tiedot siirretään rekrytointijärjestelmästä henkilöstönhallinnon puolelle ja esimies täydentää tiedot henkilöstöhallinnon järjestelmään. Henkilön tiedot siirretään luvitusjärjestelmään (eräajopohjaisesti). Luvitusprosessi käynnistyy, kun ehdot täyttyvät ja henkilölle luodaan perusvaltuudet (mm. sähköposti, oikeudet tarvittaviin järjestelmiin) työroolin mukaisesti. Tieto valtuuksien luomisesta lähetetään esimiehelle, joka tarvittaessa käy vielä hyväksymässä työntekijälle luodut käyttöoikeudet.
5. Työ alkaa ja palkanmaksu käynnistyy. Henkilölle on luotu perusvaltuudet työroolin mukaisesti ennakoidusti (käyttäjätunnukset ja salasanat tarvittaviin kohdejärjestelmiin ovat työntekijän käytössä). Tarvittaessa henkilö tai hänen esimiehensä hakee lisävaltuuksia työtehtävien suorittamiseksi. Palkanmaksun onnistumisen kannalta on kriittisiä päiviä, joita ennen tulee tiedot olla kirjattuna järjestelmään ja tämä tulee ottaa huomioon tietoja tallennettaessa ja siirrettäessä.
6. Työ käynnistyy sovittuna päivänä. Käyttäjän käyttövaltuudet tulee olla aktiivisina työn käynnistyessä.
7. Sovitaan lopetuspäivä. Henkilön käyttövaltuudet passivoidaan päättymispäivänä. Työvelvoite saattaa päättyä jopa kuukausia ennen palkanmaksun päättymistä.
8. Henkilön työsuhde päättyy. Työvelvoite saattaa päättyä jopa kuukausia ennen palkanmaksun ja työsuhteen päättymistä.
9. Palkanmaksu päättyy, viimeiset maksut suoritetaan, henkilön työsuhde voidaan poistaa ja historioida.

Työsuhteen tai työvelvoitteen välitön purkaminen normaalissa työsuhteessa:

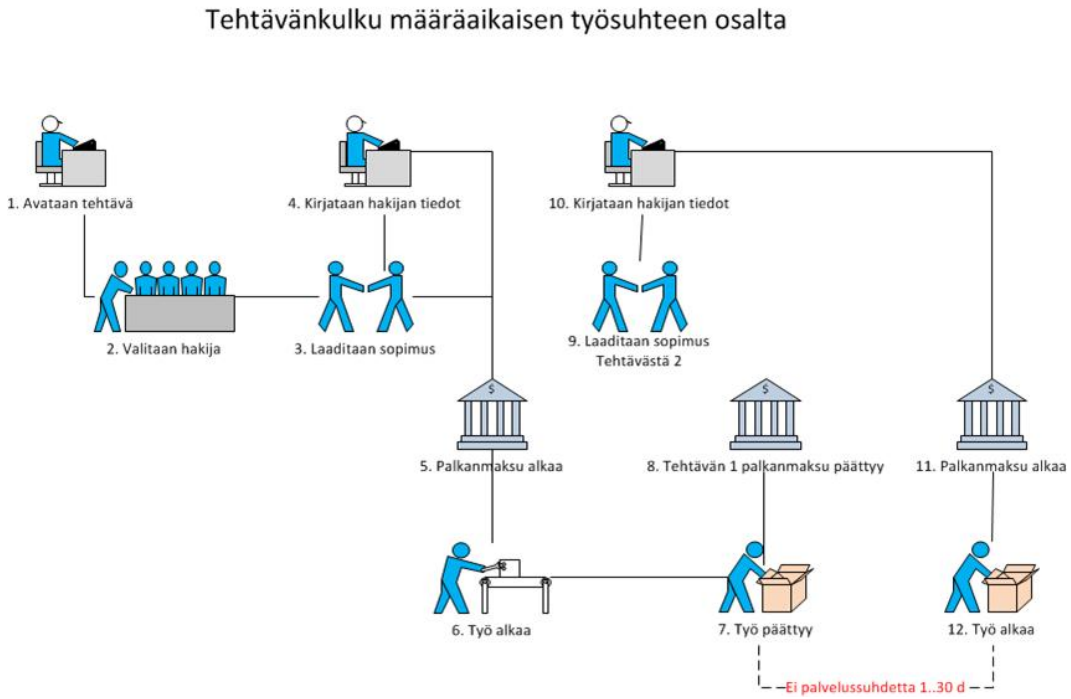
6. Stepit 1-6 kuten normaalissa työ suhteessa
7. Työnantaja saa purkaa työsuhteen heti laissa määriteltyjen painavien syiden perusteella. Myös työntekijälle on laissa määritelty oikeus purkaa vastaavasti työsuhde.
8. HR päivitykset ja muutokset ajetaan eräajona. Työvelvoitteen välittömässä purkamisessa on tarve estää henkilön pääsy järjestelmiin ja poistaa valtuudet heti sekä estää henkilön näkyvyys jakelulistoilla. Tähän on eri keinoja:
   a) Manuaalisesti kaikkiin kohteisiin, manuaalinen ohjaus
   b) Käyttövaltuushakemiston suora päivitys, josta provisiointi heti: Päivitettäviä tietoja ovat mm:
      - henkilön tila
      - käyttövaltuushakemiston tilatieto

- Organisaatiokohtainen ohjauskoodi (ohjausbitti), jolla estetään eräajona mahdollisesti myöhemmin tulevat päivitykset (voisivat aktivoida tilanteen väärin)

Sama prosessi ” lepäävässä työsuhteessa”: valtuuksia ei poisteta, vaan passivoidaan Vastaavasti kuolemantapauksissa työsuhde päätyy heti.

2.2 Tehtävänkulku määräaikaisen työsuhteen osalta

Määräaikaisessa työsuhteessa, joka ei ole verrattavissa normaalin työsuhteeseen (pitkä-aikainen määräaikaisuus) henkilö toimii toisen henkilön sijaisena tai harjoittelijana. Määräaikaisuuden voivat jatkua heti toisensa perään tai niiden välissä voi olla aikajaksoja, jolloin henkilöllä ei ole sopimusta. Käyttövaltuuksia ei saisi poistaa ennen seuraavan sijaisuuden alkua, jos määräaikaisuuksien väliin jäävä aika on kohtuullinen esimerkiksi 1-30 päivää.



Kuva 2. Määräaikainen työsuhde

Määräaikaisen työsuhteen sanallinen käyttökertomus:

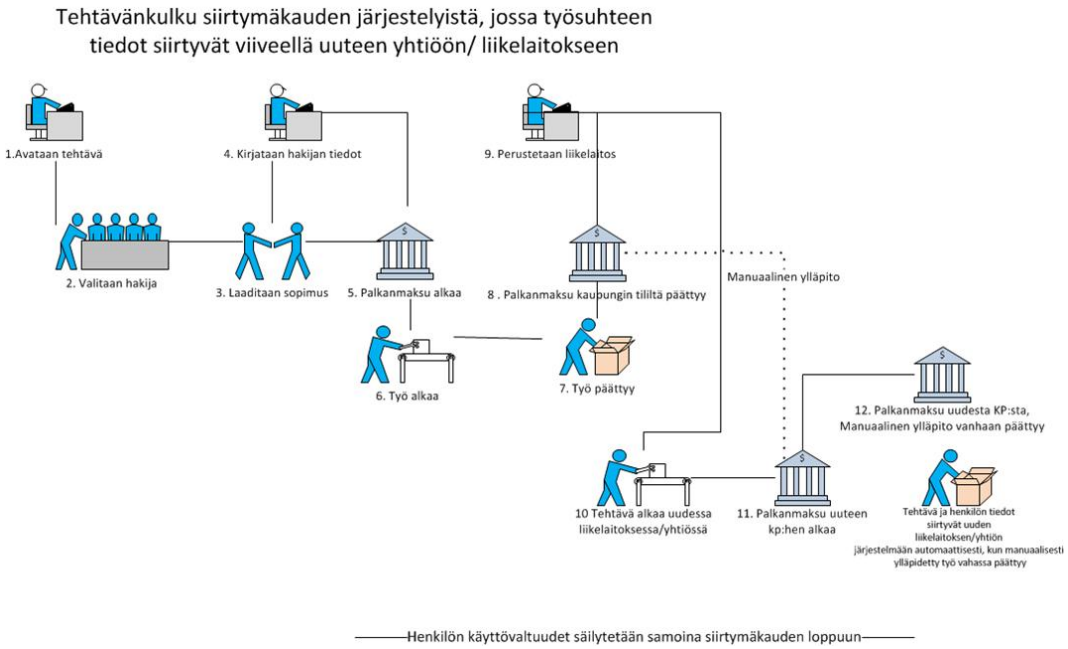
6. Stepit 1-6 kuten edellä (normaali työsuhde)
7. Henkilö saattaa toimia useamman henkilön vuorotteluvapaan sijaisena tai pitää palkattoman loman jaksojen välissä, jolloin ensimmäinen työsuhde päättyy ja

uusi alkaa. Tällöin samaksi käyttövaltuudeksi yhdelle henkilölle voidaan tulkita tilanteita, joissa poissaolo (työsuhteen päättymisen ja uuden alkamisen välinen aika) kestää 1-30 päivää jaksojen välissä

8. Työsuhde 1 päättyy, sovitaan lopetuspäivä. Mikäli on tarvetta jatkaa määräaikaista työsuhdetta, päivitetään sopimusta vastaavasti, jolloin lopetuspäivä siirtyy.
9. Palkanmaksu työsuhteesta 1 päättyy. Työntekijää ei poisteta. Työntekijän oikeudet voidaan laittaa lepotilaan (30 päiväksi), kunnes tehtävä 2 mahdollisesti käynnistyy. Työtekijän käyttövaltuudet poistetaan/ passivoidaan määräajan umpeuduttua, jos ei uutta määräaikaisuutta sovita.
7. Esimies kirjaa työntekijän tiedot ja työntekijälle uuden työroolin. (Työntekijän kanssa voidaan sopia toisesta työtehtävästä jo ennen määräaikaisuuden päättymistä työsuhteessa 1). Sopimuksessa sovitaan aloituspäivä. Esimies tarkistaa mahdollisesti syntyvät vaaralliset työyhdisteet. Henkilön yksilöivä tunniste ja tiedot ovat olemassa. Luvitusprosessi ylläpitää uuden työroolin mukaiset oikeudet ja provisoi tarvittaviin järjestelmiin aikataulun mukaisesti.
8. Palkanmaksu alkaa sopimuksen mukaisesta päivästä alkaen
9. Työ tehtävässä 2 alkaa sopimuksen mukaisena päivänä, jolloin työroolin mukaiset valtuudet ovat käytettävissä.

2.3 Tehtävänkulku siirtymäkauden järjestelyistä

Alla on kuvattu tehtävänkulku siirtymäkauden järjestelyistä, jossa työsuhteen tiedot siirtyvät viiveellä uuteen yhtiöön/ liikelaitokseen. Erityisesti uusien liikelaitosten kohdalla tilanne toistuu, kun vastaanottava kohde ei ole vielä saanut käyttöympäristöään valmiiksi kaikilta osin. Näissä tilanteissa tulee pystyä asettamaan henkilön poisto manuaaliseksi, kunnes vastaanottava organisaatio pystyy perustamaan tehtävän omiin järjestelmiinsä. . Tässä kuvattu järjestely poistaa normaaliprosessin käytöstä, joten tällöin kannattaa siirtymäaika pitää mahdollisimman lyhyenä.



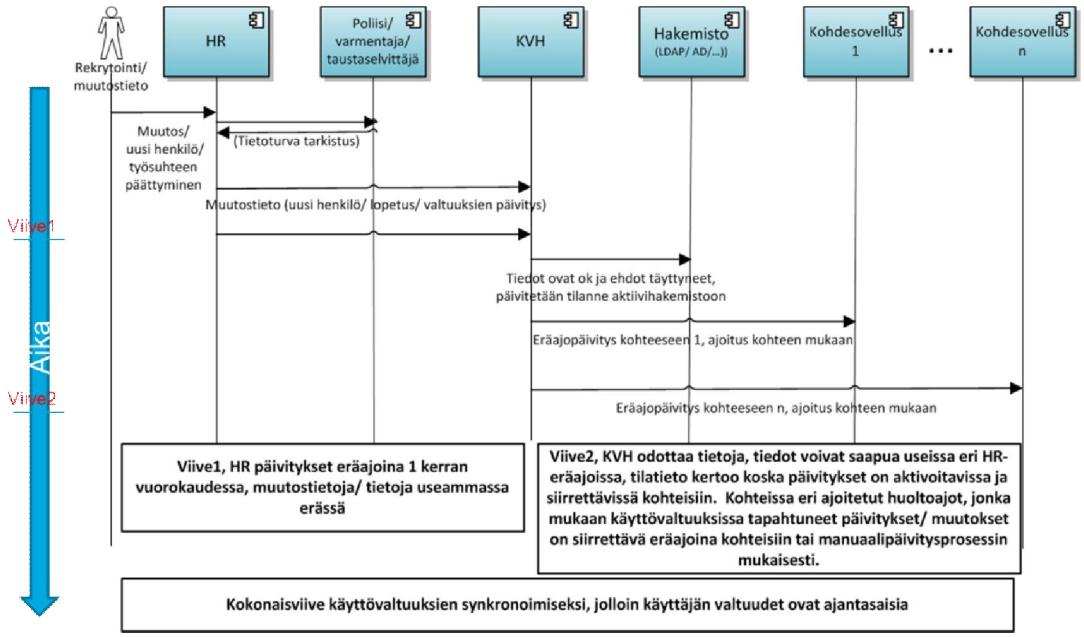
Kuva 3: Siirtymäkauden järjestely työsuhteessa

Siirtymäkauden aikaisen työsuhteen sanallinen käyttökertomus:

6. Stepit 1-6 kuten edellä (normaali työsuhde)
   Työ kaupungin työntekijänä päättyy. Siirtymän hidastaminen ja poiston estäminen pitää aina määritellä ja toteuttaa erikseen ennakkoon. Poikkeustilanteen pitkittyessä tulee ongelmia tietojen päivityksessä, kun henkilöiden poisto on estetty normaalijärjestelyin
7. Palkanmaksu kaupungin työntekijänä päättyy
8. Perustetaan uusi liikelaitos, johon työntekijän tiedetään siirtyvän.
9. Työ uudessa liikelaitoksessa alkaa. Henkilön käyttövaltuudet säilytetään samoina siirtymäkauden loppuun ja ylläpidot hoidetaan manuaalisesti.
10. Palkanmaksu uudessa liikelaitoksessa alkaa
11. Tehtävä ja henkilön tiedot siirtyvät uuden liikelaitoksen/yhtiön järjestelmään automaattisesti, kun manuaalisesti ylläpidetty työ vahassa päättyy. Palkanmaksu tapahtuu uuden kustannuspaikan kautta.

3 Aikakaaviot

Henkilön palvelussuhteeseen ja valtuuksiin liittyvien tietojen siirtoja varten tulee määritellä aikakaavio. Aikakaaviossa otetaan huomioon eri järjestelmien väliset päivitysajot, kohdejärjestelmien ”huolto-ikkunat”, joiden puitteissa päivitykset valtuutusmuutokset tulee tehdä. Myös manuaalisten päivitysten yhteydessä on huomioitava päivityspyynnön läpimenoaika, jotta pystytään laskemaan kokonaisaika, jolla valtuutukset ovat kaikkialla oikea-aikaisia. (katso kuva alla)



Kuva 4: Aikakaavio muutosten läpiviemiseksi. Alkaa havaitusta muutoksesta tai uuden henkilön saapumisesta ja päättyy, kun valtuudet ovat ajantasalla.

Viive 1: määräytyy tilanteen mukaan:

- Uudet henkilöt, tehdäänkö heille taustalla varmennus, jonkun ulkopuolisen varmentajan kautta, vai ei.
- Miten usein HR:n eräajot käynnistyvät.
- Kuinka monessa HR:n eräajossa saadaan kaikki tarvittava tieto käyttövaltuuksien hallitsemiseksi.

Viive 2:määräytyy myös tilanteen mukaan:

- Käyttövaltuuksien hallinta tarkistaa ovatko kaikki tiedot saapuneet ja ovatko ehdot täyttyneet tietojen päivittämiseksi hakemistoon ja kohdejärjestelmiin
- Tiedot päivitetään hakemistoon

- Tiedot päivitetään kaikkiin tarvittaviin kohdejärjestelmiin eri tavoin:
  - Manuaalisesti kaikkiin, työroolin/ pyyntöjen mukaisesti
  - Automaattisesti provisioiden osaan kohdejärjestelmistä ja osaan manuaalisesti työroolin/ pyyntöjen mukaisesti
  - Automaattisesti provisioiden työroolin mukaisesti.
- Aika, joka kuluu kohdejärjestelmiin päivittämiseksi, vaihtelee tavista riippuen.

Liite 3

Ohjelmisto- Rooli oikeudet matriisi (oikeudet rooleittain)

Versio x.x Päivitetty pp.kk.vvvv		Rooli 1	Rooli2	Rooli 3				
ohjelmisto 1		tunnukset ja oikeudet		tunnukset ja oikeudet				
ohjelmisto 2			tunnukset ja oikeudet					
Ohjelmisto 3		tunnukset ja oikeudet						

Liite 4

Kuntasektorin arkkitehtuuriryhmä

Kuntasektorin käyttövaltuushallinnan viitearkkitehtuuri

Versio 1.0

Eteneminen

Helsinki 2013

Kuntaliitto
Kommunförbundet

Sisältö

Johdanto

Tämä kuvaus on tarkoitettu käytettäväksi esimerkinomaisena etenemisen ohjeena mietittäessä käyttövaltuushallinnan toteuttamista kunnan toimintaympäristöön. Etenemisprosessin avulla voidaan hahmottaa ongelmakohdat, jotka liittyvät käyttövaltuushallinnan ratkaisun toteuttamiseen ja jatkuvaan hallintaan sekä ylläpitoon. Kunnan tulee omien lähtökohtien puitteissa toteuttaa käyttövaltuushallinta, ratkaista mitkä järjestelmät kuuluvat sen piiriin ja mihin kohderyhmiin se toteutetaan. Olennaista on tunnistaa kunnan koko toimintaympäristö käyttövaltuushallinnan näkökulmasta ja edetä siinä sopivin askelin. Koko käyttövaltuushallinnan toteuttaminen kerralla ei ole suositeltavaa.

2 Taustaa

Käyttövaltuushallinta (IAM – Identity and Access Management)) voidaan osittaa karkeasti osiin (katso kuva alla), jotka ovat toteutettavissa vaiheittain:

Kertakirjautuminen

- Koko organisaation laajuinen kertakirjautumisen ratkaisu. joka kattaa kokonaan tai lähes kokonaan organisaation tietojärjestelmäpalvelut

Identiteetin ja käyttövaltuuksien hallinta

- Pääsyn-, käyttäjävaltuuksien sekä identiteettien hallinta

Kuva1: Käyttövaltuushallinnan osakokonaisuudet

Tarkemmin kokonaisuudessa on tunnistettavissa eri määrittelykerrokset - tuotepaketit, joita on kuvattu seuraavassa kuvassa, alla.

Kuva 2: Käyttövaltuushallinta tuotepaketit

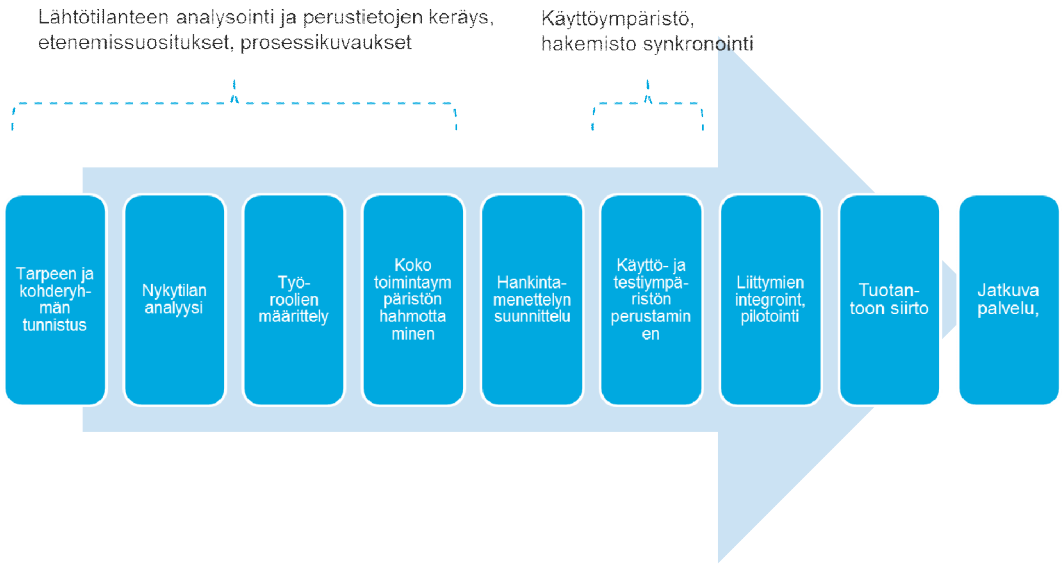
KVH (IAM) hankkeen yhteydessä määritellään suuntaviivat yhteiselle päähakemistolle, johon tarjotaan liitosmahdollisuutta KVH käyttöönottoa suunnitteleville kunnille. Yhteinen hakemistorakenne ja nimeämiskäytännöt mahdollistavat palveluiden keskitetyn hallinnan ja jakelun laajalle käyttäjämäärälle. Hakemisto on otettavissa vaiheittain asiakkaiden käyttöön halutun laajuisena kokonaisuutena.
Yhteisellä hakemistorakenteella on saatavissa merkittäviä kustannussäästöjä

3 Eteneminen

Etenemisessä on ensin etenemisprosessi ja sitten karkea aikataulu, jossa etenemisprosessin mukaiset tehtävät on otettu huomioon.

3.1 Etenemisprosessi

Eteneminen kuvataan karkealla tasolla, koska etenemiseen vaikuttaa kunnan koko, kunnan tila ja kypsyystaso käyttövaltuushallinnan suhteen.
Etenemisen karkean tason prosessikuvaus kuvaa toiminnallisuuden tarkemmin, joka on tuotepakettien takana.



Kuva x: Etenemisen prosessi

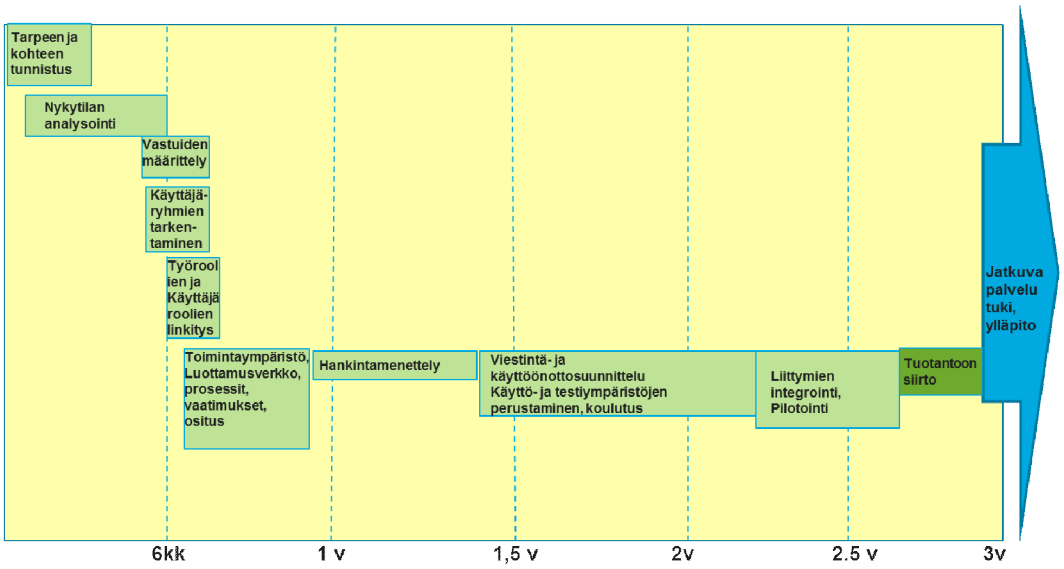
Vaihe	Kuvaus	Tiedot/Tulos
Tarpeen ja kohderyhmän tunnistus	Kohteen ja kohderyhmän rajaus • Mille kohderyhmälle tai kohderyhmille käyttövaltuushallintaa ollaan tekemässä/rajaamassa. Esimerkiksi rajaudutaanko sisäisiin henkilöihin/ koko henkilöstö, ulkoisiin henkilöi-	Kohde on rajattu Tavoitteet määritelty ja kuvattu

	hin, luottamushenkilöihin ja heidän vahvaan tunnistamiseen, valittuun toimialaan, tunnettuihin laitteisiin, pääsynhallinta verkkoon Tavoitteet, joita voivat olla: • Poistot: on havaittu, että ympäristöön jaa tuntemattomia käyttäjiä roikkumaan. Tavoitteena on ylimääräisten henkilöiden ja heidän valtuuksien poisto hallitusti • Luonti: Uusien henkilöiden ja heidän valtuuksien luonti hallitusti ympäristöön • Luvitus: uusien henkilöiden luvitus ympäristöön (vrt. luonti), roolien muutokset, roolien valtuuksien muutokset helposti ja hallitusti ympäristöön • Delegointi: Oikeuksien/ vastuiden siirto toiselle henkilölle itsepalveluna • Auditointi: auditointiperiaatteet, tasalaatuista ja jäljitettävää lokiin kirjoitusa	
Nykytilan analyysi	Tehdään nykytila-analyysi rajoittuen edellä rajattuihin tavoitteisiin Varmistetaan edellytysten täyttyminen Tehdään gap-analyysi nykytilan ja tavoitteiden suhteen Arvioidaan kyvykkyys muutosten läpiviemiseksi ja tehdään alustava ehdotus etenemiseksi	vaikutus (gap) -analyysitulos etenemissuunnitelma ehdotus
Työroolien määrittely	Työroolien ja työrooliin liittyvien valtuuksien määrittely työroolien ja järjestelmien käyttäjäroolien linkitys	työrooli-käyttäjärooli matriisi
Koko toimintaympäristön hahmottaminen	Toimintaympäristön kokonaiskuvan hahmottaminen Luottamusverkko, luottamusverkkohierarkian määrittely Prosessien mallinnus tavoitteen mukaisen rajatun kokonaisuuden näkökulmasta Vaatimusten kartoitus ja kokoaminen mukaan lukien tarvittava ympäristö Kokonaisuuden ositus/ vaiheistus	Toimintaympäristön kokonaiskuva Luottamusverkko ja sen hierarkia määritelty Prosessit mallinnettu Vaatimukset kirjattu Ositus/Vaiheistus kuvattu
Hankinta-menettelyn suunnittelu	Suunnitellaan ja päätetään miten hankitaan tavoitteen mukainen kokonaisuus eli miten eri osat vaiheistetaan omiin kokonaisuuksiin	Hankinta valmisteltu Kilpailutus tehty
Käyttö- ja testiympäristön perustami-	Suunnitellaan ja laaditaan viestintä- ja käyttöönottosuunnitelmat	Viestintä- ja käyttöönottosuunnitel-

nen	Käyttö- ja testiympäristöjen perustaminen (lisenssit, laitteet, jne.) käyttöönottosuunnitelman mukaisesti. Hakemistorakenteiden määrittely	ma Käyttö- ja testiympäristöt pystytetty Hakemistorakenne valmis
Liittymien integrointi, pilotointi	Liittymien integrointi tavoitteiden mukaisesti Ympäristön ja hankinnan osakokonaisuuden pilotointi Koulutukset	Koulutukset käynnissä Pilotointi suunniteltu ja käynnissä Tarvittavat liittymät integroitu
Tuotantoon siirto	Tuotantoon siirto käyttöönottosuunnitelman mukaisesti Tarvittavat koulutukset	Jatkokoulutukset käynnissä Tuotantoon siirto tehty
Jatkuva palvelu	Jatkuvan palvelun tuottaminen (sopimukset hankintamenettelyn aikana), tuki ja ylläpito	Sopimuksen mukainen: • Tuki toiminnassa • Ylläpito toiminnassa

3.2 Etenemisaikataulu

Etenemisaikataulussa on kuvattu keskimäärin kokemuksen perusteella etenemisprosessin mukainen etenemisaikataulu. Aikatauluun vaikuttaa suuresti kunnan koko, kunnan toimintaympäristö ja kunnan kypsyystaso/kyvykkyys käyttövaltuushallinnan toteuttamiseksi sekä kohteen rajaus (ositus sopiviin palasiin). Aikataulu on vain suuntaa antava.
Etenemisaikataulussa on otettu huomioon käyttövaltuushallinnan kokonaisuus.



Kuva X: Etenemisaikataulu

Liite 5

Kuntasektorin arkkitehtuuriryhmä

Kuntasektorin käyttövaltuushallinnan viitearkkitehtuuri

Versio 1.0

Sanasto

Helsinki 2013

Kuntaliitto
Kommunförbundet

Termi tai lyhenne	Englanniksi	Määritelmä tai selitys	Synonyymi/ huomautus
Attribuutti	attribute	käsitteeseen liittyvä ominaisuus. Esim.henkilöön liittyvä tieto	
E-SSO	enterprise single sign-on	kertakirjautuminen silloin, kun se kattaa kokonaan tai lähes kokonaan organisaation tietojärjestelmäpalvelut	
Federaatio	Federation	Kahden tai useamman operaattorin välinen tai laajempi verkosto, jossa luotetaan alkuperäisen identiteetin haltijan tunnistamismenetelmiin.	
IAM	identity and access management	identiteetti- ja käyttövaltuushallinto (sateenvarjokäsite sisältäen myös pääsynhallinnan)	KVH
identiteetti- ja käyttövaltuushallinto	identity and access management	toimintaprosessit, säännöt, organisaatio ja välineet, joiden avulla hallinnoidaan tietojärjestelmien asianmukaista käyttöä	
IdM	identity management	käyttäjähallinta, identiteettien hallinta	
IT-rooli	IT role	käyttäjälle palvelujärjestelmässä annettu käyttöoikeuksien joukko (käytetään myös nimeä järjestelmärooli)	
kertakirjautuminen	single sign-on (SSO)	pääsynvalvonnan toteutustapa, jossa käyttäjä pääsee yhdellä tunnistautumisella kaikkiin saman pääsynvalvonnan piirissä oleviin palveluihin ja resursseihin käyttövaltuuksiensa puitteissa	

Termi tai lyhenne	Englanniksi	Määritelmä tai selitys	Synonyymi/ huomautus
käyttäjä	user	organisaation työntekijä (sisäinen-ulkoinen), harjoittelija, opiskelija, asiakas tai organisaationsa toimintaan muulla tavoin liittyvä henkilö(esim. luottamushenkilö), joka käyttää palveluntarjoajien tarjoamia palveluja	
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 (IT-rooli).	
käyttäjäidentiteetti	user identity; principal identity (Liberty Alliance)	käyttäjätilin yksilöivä käyttäjän ilmentymä verkkopalvelussa	
käyttövaltuudet	usage rights, access rights, authorizations	tietojärjestelmän käyttäjälle tai esimerkiksi tietyn käyttäjäroolin omaavalle käyttäjäryhmälle myönnetyt yksilöidyt oikeudet nimettyjen palveluelementtien tai muiden resurssien käyttöön. Käyttövaltuudet määrittelevät, miten ja millaisilla edellytyksillä käyttäjällä on oikeus käyttää ao. palveluelementtejä.	
kotiorganisaatio	home organisation	yhdistettyjä identiteettejä käyttävässä toimintaympäristössä (luottamusverkoston jäsen) osapuoli, joka vastaa (organisaationsa)käyttäjän todentamisesta/ tunnistamisesta ja välittää tunnistusselosteen palveluntarjoajalle vrt. tunnis-	

Termi tai lyhenne	Englanniksi	Määritelmä tai selitys	Synonyymi/ huomautus
		tuslähde	
luottamusverkosto	circle of trust, trust circle,	"joukko palveluntarjoajia ja tunnistajia, joiden kanssa käyttäjät voivat asioida turvallisesti kuin yhdessä ympäristössä." Luottamusverkoston jäsen on sopimussuhteinen ja voi toimia luottamusverkostossa kotiorganisaationa tai palveluntarjoajana	federaatio
luvitusprosessi		käyttövaltuuksien haku-, hyväksymis- ja luontiprosessin toteuttava osa (järjestelmä), johon on liittymät käyttäjätietoja tuottavista lähdetietojärjestelmistä (HR, muutostietojen itsepalvelu). Keskitetty käyttäjä- ja käyttövaltuushakemisto sekä automaattinen käyttövaltuustietojen provisiointi ovat prosessin osaprosesseja	
metatieto		Tekniset ja hallinnolliset tiedot, jotka kuvaavat luottamusverkostoon liittyneitä kotiorganisaatioita ja palveluntarjoajia ja heidän -tunnistuslähteitään ja palvelujaan. Esim Virtu operaattori ylläpitää Virtu luottamusverkon metatietoja	
palveluntarjoaja	(SP) Service Provider	Luottamusverkoston jäsen tai ulkopuolinen palveluntarjoaja, joka tarjoaa sähköisiä palveluja kotiorganisaatioiden tunnistamille-käyttäjille.	
provisiointi	provisioning	käyttäjä- ja käyttövaltuustietojen välittäminen palve-	

Termi tai lyhenne	Englanniksi	Määritelmä tai selitys	Synonyymi/ huomautus
		lujärjestelmiin	
pääsynvalvonta	access control	tiedot, toiminnot ja menettelyt, joiden avulla palvelujärjestelmän tai sen palveluelementtien käyttö mahdollistetaan vain valtuutetuille käyttäjille	
sulkulista	certificate revocation list (CRL)	Sulkulista on luettelo peruutetuista varmenteista.	
todennus	verification, authentication	1) varmistuminen kohteen todenmukaisuudesta, oikeellisuudesta tai alkuperästä 2) käyttäjän aitoudesta (henkilöllisyydestä) varmistuminen halutulla luottamustasolla Todentamisessa nojaudutaan johonkin, jota a) käyttäjä tietää, b) käyttäjällä on tai c) käyttäjä on.	autentikointi
tunnistautuminen	identification	menettely, jossa käyttäjä esittää tunnistetietonsa	
tunnistuslähde	(IdP) Identity Provider Service	Fyysinen palvelu, joka tuottaa palvelun tarjoajille SAML yhteyskäytännön mukaisia tunnistusselosteita.	
tunnistusseloste	assertion	tunnistajan palvelujärjestelmälle toimittama selvitys, joka sisältää todennettua käyttäjäidentiteettiä vastaavia tietoja ao. käyttäjästä	
työrooli	business role	käyttäjän toimenkuvaan työorganisaatiossaan kuuluvat tietotarpeet ja toiminta-	

Termi tai lyhenne	Englanniksi	Määritelmä tai selitys	Synonyymi/ huomautus
		valtuudet	
ulkopuolinen palve-luntarjoaja	(ASP)	Yritys/ulkopuolinen yhteisö, joka tarjoaa yhteiskäyttöisiä palveluita kunnille.	
varmenne	Certificate	Digitaalisesti allekirjoitettu tietojoukko, jota käytetään luottamusverkoston palve-linten ja niiden välisten viestien aitouden, eheyden ja luottamuksellisuuden varmistamiseen.	
varmentaja	Certificate Autho-rity	Organisaatio, joka antaa varmenteita palveluille, pal-velimille ja myös henkilöille.	
valtuutus	authorization	todennetulle käyttäjälle an-nettu lupa tietyn tiedon, suojattavan kohteen tai muun palveluelementin käyttöön voimassa olevien pääsynvalvontatietojen pe-rusteella	Auktorisointi
web-kertakirjautuminen	web single sign-on (web-SSO)	organisaation selainkäyttöi-siä palveluja koskeva kerta-kirjautumisympäristö/-järjestelmä	