SARKK-käyttäjähallinta

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Visamäki, Tietojenkäsittelyn koulutus

kevät 2017

Jaana Koivisto

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutus
Visamäki

Tekijä Jaana Koivisto **Vuosi** 2017

Työn nimi SARKK-käyttäjähallinta

Työn ohjaaja/t Tapani Rinne

TIIVISTELMÄ

Tässä opinnäytetyössä tutkitaan käyttäjähallinnan rakentamista sähköisen arkistoinnin järjestelmään. Tavoitteena on rakentaa roolipohjainen käyttäjähallinta, joka olisi mahdollisimman joustava, helppokäyttöinen ja pitkäikäinen. Roolipohjaisuudella tässä työssä tarkoitetaan käyttöoikeuksien antamista työtehtävien perusteella tehtäväluokkiin. Rooli voi olla esim. titteliin, työnkuvaan tai asemaan perustuva.

Teoriaosuudessa keskitytään asianhallinnan perusteisiin ja selvitetään asianhallinnan merkitys ja tavoitteet organisaatiossa. Arkistoinnista kirjoitettaessa keskitytään nykyisen tilan kuvaamiseen ja tavoitteisiin sähköisen arkistoinnin osalta. Sähköisestä arkistoinnista löytyy vielä toistaiseksi vähän tietoa, koska asia on vasta tulossa kuntiin. Selvitetään myös mihin käyttäjähallintaa tarvitaan ja mihin roolipohjaisella käyttäjähallinnalla pyritään.

Asiakastapauksena on Salon kaupungissa käyttöön otettu SARKK-palvelu ja sen käyttäjähallinta. Koska organisaatiomuutokset ovat viime vuosina olleet jatkuvia, opinnäytetyössä mietitään miten rakennetaan mahdollisimman pitkäikäinen ja helppokäyttöinen roolipohjainen käyttäjähallinta palveluun. Lopputuloksena esitellään tapa rakentaa käyttäjähallinta Salon tarpeisiin.

Avainsanat Asianhallinta, sähköinen arkistointi, käyttäjähallinta

Sivut 20 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Information Technology
Visamäki

Author Jaana Koivisto **Year** 2017

Subject Access Rights Management for SARKK

Supervisor Tapani Rinne

ABSTRACT

The purpose of this thesis was to explore how to build an access based management for electronical archiving. The goal is to build a role-based access management which is flexible, user-friendly and long lasting. The role-based means access rights which are based in worker's job tasks and is given with the classifications of the functions of municipality (COFOG). Role can be based in job title, job description or post.

In the theoretical part of the thesis, the basic knowledge of document management, the purpose of it and the goals for it are described. The archiving part contains what the situation is now and what is wanted from electronical archiving. Because electronical archiving has not been taken in use in many municipalities, there is not much knowledge of it. Part of this thesis is exploring the meaning of access-right management and where we get with it.

The customer case of this thesis is a project of SARKK, a service of electronical archiving and the access right management of it. There are always continuous changes in organisation, so there must be a long lasting and user friendly way to maintain the role-based access management. In the end of this thesis, one way to build it is presented.

Keywords Document management, electronical archiving, access management.

Pages 20 pages

SISÄLLYS

1 JOHDANTO

Julkishallinnon sähköisten asiakirjojen sähköiseen pitkäaikaissäilyttämiseen on tarjolla kansallisen ns. SÄHKE-normin täyttäviä sähköisen arkistoinnin palvelujärjestelmiä. Yksi näistä on SARKK, joka automatisoi asiakirja-aineiston hallintaa vastaanottamisesta aina hävittämiseen asti. Palvelun avulla aineisto voidaan arkistoida määräajaksi tai pysyvästi ja samalla nopeutetaan asiakirjojen käsittelyä ja hakua. Sähköisten asiakirjojen ja asioiden luokittelun perustana on kansallisesti käytetty ns. kuntien yhteinen tehtäväluokitus. Asiakirjat tuotetaan tietyssä tehtävässä. Tehtäväluokitusta voidaan käyttää myös sähköisessä arkistopalvelussa käyttöoikeuksien antamiseen. Tässä opinnäytetyössä tutkitaan, millä tavalla käyttäjähallinta kannattaa rakentaa, että se olisi mahdollisimman pitkäaikainen muuttuvassa organisaatiossa.

SARKK-palvelu eli Sähköinen Arkistointi Kuntien Käyttöön on tarkoitettu aineistolle, jota pitää säilyttää määräaikaisesti tai pysyvästi. SARKK-palvelu on osana Kuntien Tiera Oy:n palvelusalkkua. Teknisestä toteutuksesta vastaa Fujitsu Finland Oy, joka huolehtii palvelun toiminnasta SaaS-pilvipalveluna (Software as a Service). SARKK-arkisto perustuu EMC Documentum–ratkaisuun (Fujitsu 2012).

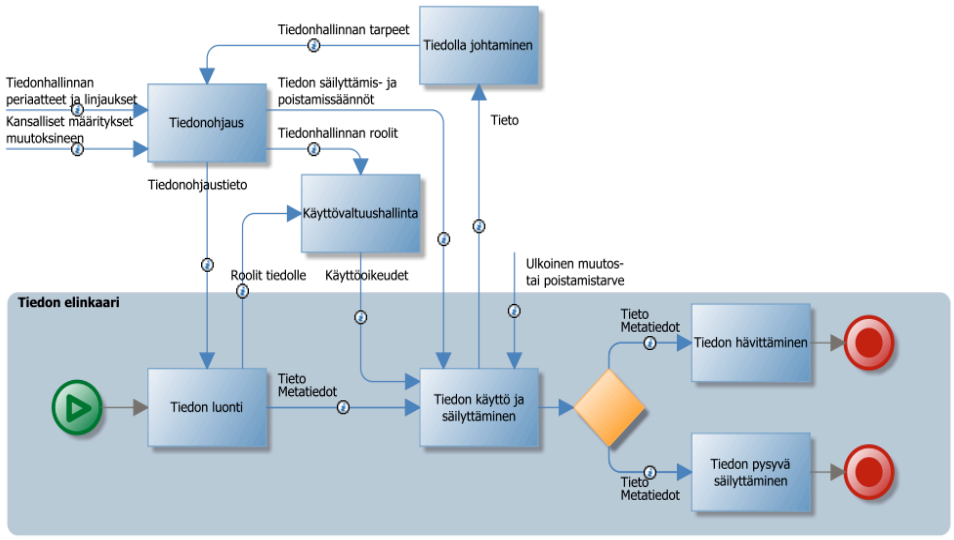
Opinnäytetyön teoreettisessa osiossa käydään läpi asiakirjahallinnan perusteita aina sähköiseen arkistointiin asti. Käyttäjähallinnan ja varsinkin roolipohjaisen käyttäjähallinnan merkitys tuodaan teoreettisessa osiossa myös esille.

Empiirisessä osiossa sovelletaan tietoja ja tutkitaan, minkälainen käyttäjähallinta soveltuu sähköisen arkistoinnin hallintavälineeksi. Tutkimusosiossa tutkitaan myös eri tapoja rakentaa käyttäjähallinta ja pohditaan eri ratkaisujen vaikutuksia muutostilanteessa. Lopputuloksena esitellään suositeltu tapa tehdä käyttäjähallinta SARKK-palveluun.

2 ASIANHALLINTA

Suomessa asiakirjojen järjestäminen arkistossa tapahtuu provienssiperiaatteella. Keskeinen ajatus on, että eri arkistonmuodostajien asiakirjat säilytetään omana kokonaisuutenaan. Tämä vahvistaa asiakirjojen todistusvoimaisuutta ja yhdistää asiakirjat laajempiin kokonaisuuksiin (Intranet, Salon kaupunki).

Suomessa asianhallinta perustuu elinkaariajatteluun, eli jokaisen asiakirjan vaiheet muodostavat kokonaisuuden. Asiakirjan saapuminen, arkistointi ja säilyttäminen ovat asianhallinnan eri vaiheita. Julkishallinnon asianhallintaa ohjataan arkistonmuodostussuunnitelmalla (AMS). Kun siirrytään sähköiseen asianhallintaan, käytetään nimitystä tiedonohjaussuunnitelma (TOS). Julkishallinnon asiakirjahallintaa ohjataan Arkistolailla (831/1994). Kunnan asiakirjahallinnan tehtävänä on huolehtia asiakirja-aineiston säilyvyydestä ja käsittelystä asiakirjan koko elinkaaren ajan sekä tietopalvelun, tietosuojan ja tietoturvan varmistamisesta.

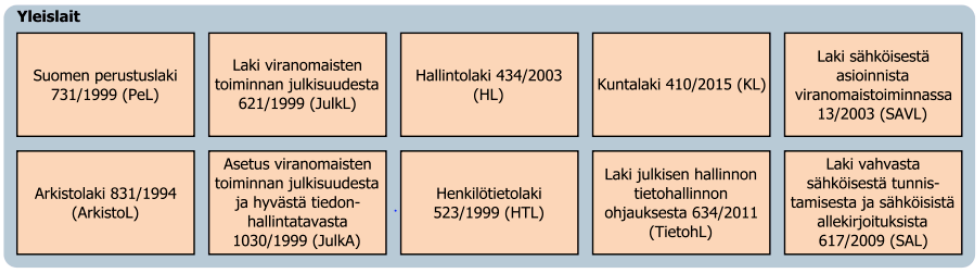


Kuva 1. Tiedon elinkaarihallinta (Kunnat.net 2016)

Kunnissa syntyvä tieto tallennetaan tietojärjestelmään. Järjestelmästä tieto on oikeutettujen käyttäjien saatavilla tehtävien suorittamiseen ja asioiden käsittelyyn. Tallennuksen yhteydessä lisätään tietoa kuvailevat metatiedot joiden avulla hallitaan tiedon saatavuutta ja elinkaarta (Kuva 1).

Tiedonhallintaa säätelevät kunnissa monet lait ja asetukset (Kuva 2). Arkistolaki, julkisuuslaki ja henkilötietolaki ovat iso osa tiedonhallinnan kehittämisessä. Hyvä tiedonhallintatapa edellyttää, että julkisuus, asiakirjahallinto, tietoturva, tietosuoja ja sähköinen asiointi ovat hyvin organisoitu ja ohjeistettu. Henkilötietojen käsittelyn tulee olla laillista, hyvän tietojenkäsittelytavan mukaista, suunnitelmallista ja sidottu käyttötarkoitukseen. Henkilötietolaki sisältää määritykset mm. henkilörekisteristä ja arkaluontoisista tiedoista (Kuntaliitto.fi 2017). Yleistä tietosuoja-asetusta (2016/679) sovelletaan 25.5.2018 alkaen. Tietosuoja-asetus kohdistuu henkilötietoihin ja henkilötietojen käsittelyyn ja sen tarkoitus on palauttaa henkilötietojen kontrolli takaisin kansalaisille sekä selkiyttää tietosuojaa koskevaa lainsäädäntöä (Tietosuoja.fi 2017).

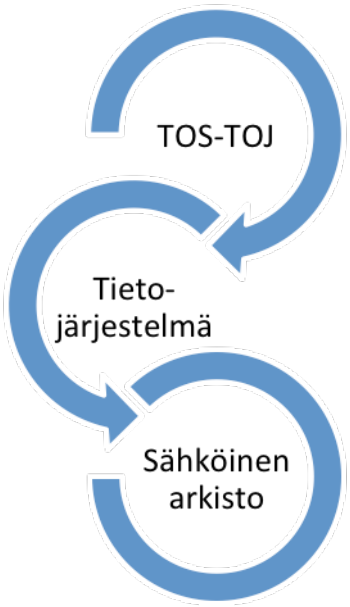
Lakien lisäksi tulevat kansallisarkiston määräykset ja ohjeet, joiden tarkoitus on ohjata ja tukea asiakirjahallintoa ja arkistotointa (Arkisto.fi 2017).



Kuva 2. Yleislait (Kunnat.net 2016)

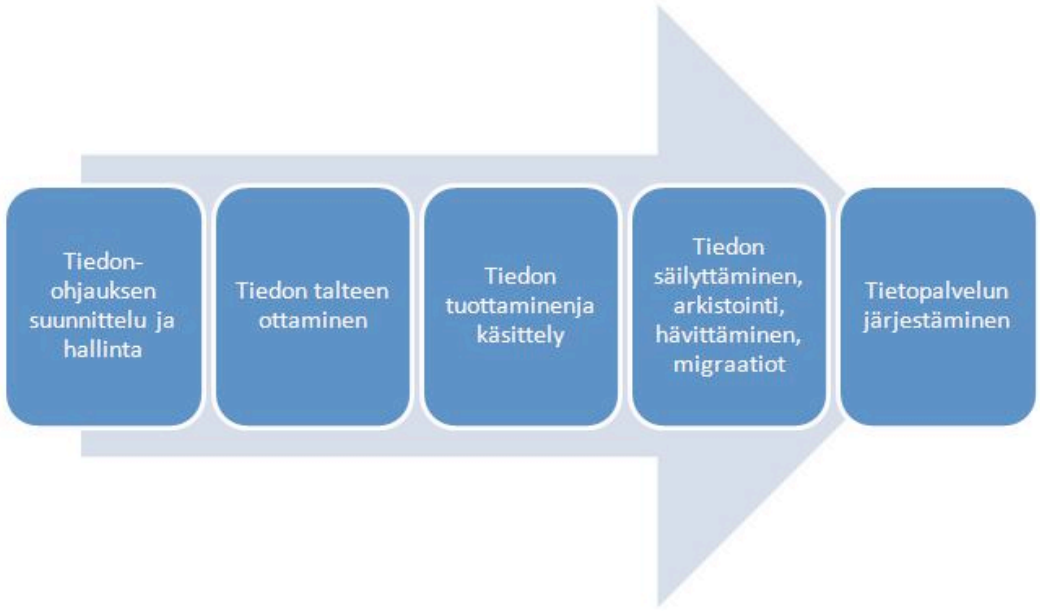
Asiakirjatiedon käsittelyä ja arkistointia ohjataan tiedonohjausjärjestelmän avulla. Asiakirja tuotetaan operatiivisessa järjestelmässä ja siirretään sähköiseen arkistoon operatiivisesta järjestelmästä tai käyttöliittymän avulla. Asiakirjoihin liitettyjen metatietojen tulee olla riittävät, jotta tiedot ohjautuvat oikeaan tehtävään, palveluun ja taustajärjestelmään (Kuva 3).

Operatiiviset järjestelmät tulee integroida rajapinnan avulla keskitettyyn tiedonohjausjärjestelmään. Kaikkia järjestelmiä ei tarvitse integroida, jos käyttöä on vähän tai järjestelmä ei sisällä pysyvästi tai määräaikaisesti säilytettävää tietoa tai jos integroinnin kustannukset ovat suuret hyötyyn nähden. Operatiiviseen järjestelmään liitetty tiedonohjausjärjestelmä määrittelee tarvittavat metatiedot. Metatiedot tuotetaan integraatiossa tai tietojen tuonnin yhteydessä rajapinnassa (Kunnat.net 2016).



Kuva 3. Sähköisen asiahallinnan mahdollistaa kolmen eri tietojärjestelmän yhteen toimiminen (Intranet, Salon kaupunki 2016)

Asiakirjahallinnon tehtävänä on määritellä mitä tietoa on tarpeellista säilyttää asiakirjoina ja mitkä metatiedot tulisi syntyä kussakin toiminnan prosessissa.



Kuva 4. Asiakirjahallinnan prosessi (Intranet, Salon kaupunki)

2.1 SÄHKE2

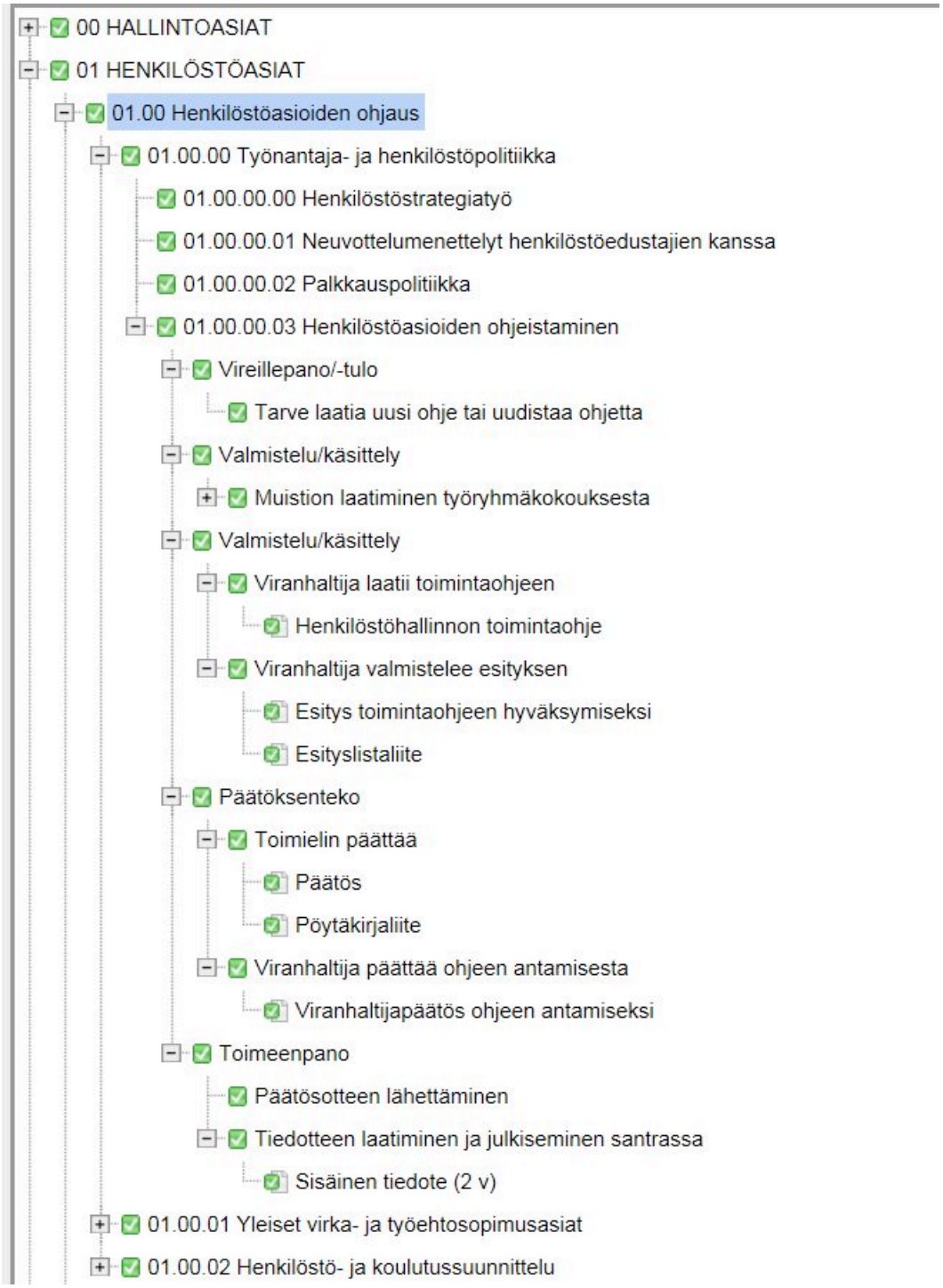
Nykyisin asiakirjahallinnon haasteet ovat sähköisessä säilyttämisessä. Asiakirjojen sähköistä säilyttämistä ohjaavat Arkistolaitoksen SÄHKE2-määräykset, joissa kerrotaan sähköisen asiakirjan käsittelystä, hävittämisestä ja tietojen säilyttämisestä. SÄHKE2-määräys astui voimaan 1.1.2009. SÄHKE2-normissa tiedonohjauksen tuottaminen on oleellisin asia. Tiedonohjauksen vaatimuksiin sisältyy, että sähköiseen tiedonohjaussuunnitelmaan määritellyt metatiedot tallentuvat tietojärjestelmiin operatiivisen käsittelyn aikana. Määräyksessä esitetään ne periaatteet, joiden mukaan TOS-ohjaus tietojärjestelmiin toteutetaan (Kansallisarkisto 2017).

2.2 Tehtäväluokitus

Kuntien yhteinen tehtäväluokitus valmistui loppuvuodesta 2008 kuntien ja kansallisarkiston yhteisenä projektina. Tarkoituksena oli, että tehtäväluokitusta käytetään organisaatiossa kolmannella tasolla ja syvennetään tarvittaessa neli- tai viisiportaiseksi. Tehtäväluokitus oli riippumaton organisaation rakenteista, tietojärjestelmistä, asiakirjoista ja nimikkeistä. Kuntien jatkokehittämisen varassa oli omien tehtävien sitominen malliin ja sähköisten toimintatapojen käyttöönotto (Kansallisarkisto 2017).

Tehtävät jaetaan päätehtäviin, tehtäviin ja alatehtäviin. Tehtäväluokitus on numeroitu niin, että ylimmällä päätehtävätasolla luokitusnumero on kaksinumeroinen, toisella tasolla nelinumeroinen ja kolmannella kuusinumeroinen. Esimerkiksi Salossa päätehtävät jaetaan neljääntoista luokkaan seuraavasti (Kuva 5):

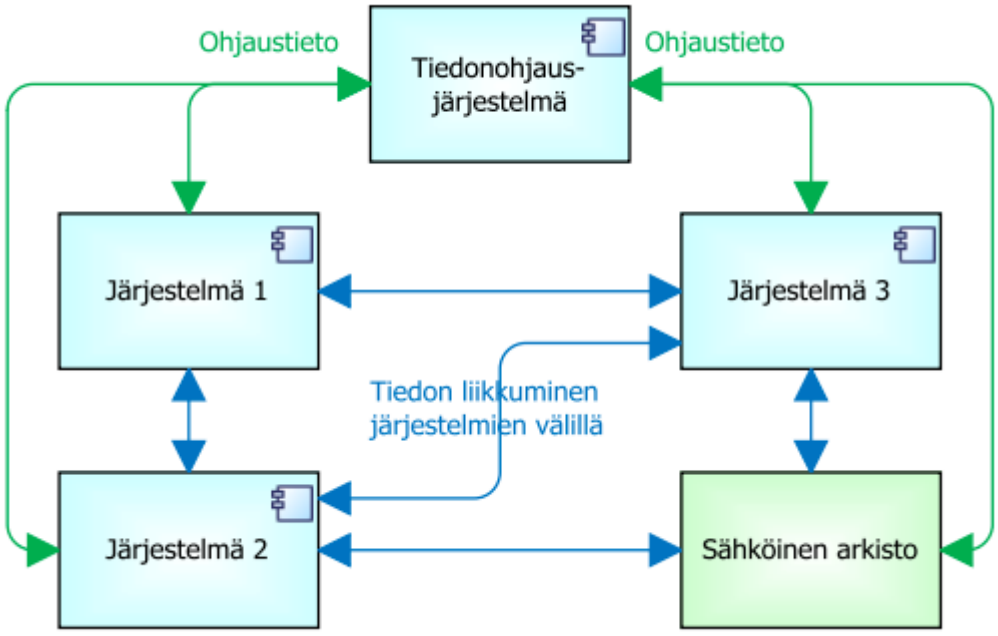
00 Hallintoasiat
01 Henkilöstöasiat
02 Talousasiat, verotus ja omaisuuden hallinta
03 Lainsäädäntö ja lainsäädännön soveltaminen
04 Ulkopolitiikka ja kansainvälinen toiminta
05 Sosiaalihuolto
06 Terveydenhuolto
07 Tiedonhallinta ja viestintäpalvelut
08 Liikenne
09 Turvallisuus ja yleinen järjestys
10 Maankäyttö, rakentaminen ja asuminen
11 Ympäristöasiat
12 Opetus ja sivistystoimi
13 Tutkimus- ja kehittämistoiminta
14 Elinkeino- ja työvoimapalvelut



Kuva 5. Esimerkki TOS-rakenteesta (Intranet, Salon kaupunki)

2.3 Tiedonohjaus

TOS eli tiedonohjaussuunnitelma on organisaation asiakirjallisten tietojen käsittelyn, rekisteröinnin ja säilyttämisen ohjeisto. Se sisältää organisaation kaikki kertyvät asiakirjat ja tietoaineistot. TOS on edellytys sähköisten asiakirjatietojen hallinnalle ja se laaditaan tiedonohjausjärjestelmässä (TOJ). Tiedonohjausjärjestelmän tehtävä on välittää metatietoarvoja, ohjaustietoja ja käsittelysääntöjä tietojärjestelmille, joissa asiakirjatietoa käsitellään (Kuva 6). Hyvää tiedonhallintatapaa on, että organisaatiolla on ajantasaiset kuvaukset omista tehtävistään ja niiden yhteydessä syntyvistä asiakirjoista. Tehtäväluokitus ei kuitenkaan korvaa prosessikuvauksia ja niiden toteutuksia, vaan se tarjoaa ohjaustietoa eri käsittelyvaiheista. Tiedonohjausjärjestelmä ja tiedonohjaussuunnitelmat ovat edellytys sähköisen arkistoinnin käyttöönotolle (Kansallisarkisto 2008).



Kuva 6. Tiedon kulku järjestelmissä (Kunnat.net 2016)

3 SÄHKÖINEN ARKISTOINTI

Sähköisessä arkistopalvelussa asiakirjatietoa hallitaan siten, että tiedon todistusvoimaisuus, luotettavuus, turvallisuus, saatavuus ja käyttökelpoisuus säilyvät asiakirjan koko elinkaaren ajan. Sähköisen asiakirjan elinkaarta ohjataan metatietojen avulla (Intranet, Salon kaupunki).

Sähköisen arkistoinnin tavoite on tehostaa tietopalvelua ja mahdollistaa pysyvästi säilytettävien asiakirjojen säilyttäminen. Tavoitteiksi on asetettu myös määräajan säilytettävien sähköisten asiakirjojen ohjattu hävittäminen, asiakirjojen käsittelykäytäntöjen yhtenäistäminen ja arkistotilan ja levytilatarpeen kasvun vähentäminen (Vtv.fi 2014).

”Kansalliseen kulttuuriperintöön kuuluvan pysyvästi säilytettävän asiakirjatiedon säilyvyys ja käytettävyys on varmistettu aineiston koko elinkaaren ajan säilytysmuodosta riippumatta” (Arkistolaitos 2009). Samaa tavoitteenasettelua ovat vahvistaneet myös tietoyhteiskuntaohjelman vuoden 2005 strategia, KuntaTIME–hanke ja Euroopan komission suunnitelmat sähköisen hallinnon kehittämisestä (Vtv.fi 2014). Arkistolaitos on myös asettanut tavoitteiksi lisätä mahdollisuuksia asiakirjojen sähköiseen käyttöön sekä ohjata asiakirjatiedon elinkaarihallintaa sähköisessä toimintaympäristössä (Arkistolaitos 2009).

Tietojärjestelmissä on oltava vähintään SÄHKE2-metatietomallissa pakolliseksi määritellyt metatiedot. Tietojärjestelmissä on oltava myös mahdollisuus tallentaa metatietoarvoja eri tallennusmuodoille. Metatiedot pitää myös pystyä suojaamaan niin, etteivät muut kuin ko. tietoihin käyttöoikeuden saavat henkilöt pääse tietoihin (Vtv.fi 2014).

Säilytysaikamääräykset ja –suositukset koskevat arkistolaissa määritettyjä asiakirjoja ja niihin rinnastettavia tietoaineistoja, joita kertyy kuntiin tehtävien hoidon tuloksena. Suositukset auttavat arkistonmuodostajia määrittämään, kuinka kauan säilytetään aineistoja joita ei tarvitse säilyttää pysyvästi. Määräykset perustuvat arkistolaitoksen päätöksen pysyvästi säilytettävistä asiakirjoista. Säilytysajat merkitään TOS:iin ja vastuu aineistojen säilyttämisestä on arkistonmuodostajalla (Kuntaliitto.fi 2002). Asiakirjat on hävitettävä luotettavasti säilytysajan umpeuduttua. Sähköisessä tietojärjestelmässä on hävitystoiminnallisuus, joka hävittää asiakirjan metatietoihin määritellyn viimeisen säilytyspäivän mukaan.

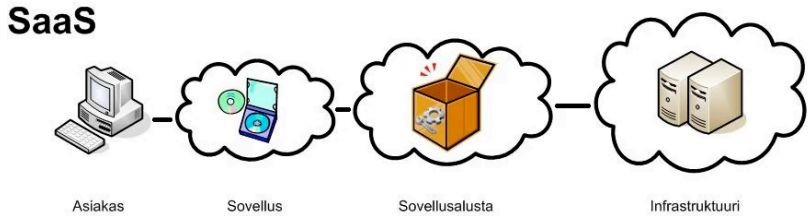
Järjestelmään luodun käyttäjähallinnan mukaan vain auktorisoidut henkilöt pystyvät luomaan, lisäämään, muuttamaan tai poistamaan tieto-

järjestelmään ja TOS:iin sisältyviä tietoja. Käyttöoikeudet annetaan käyttäjäryhmille ja niiden on vastattava henkilöiden työtehtäviä. Käyttöoikeudet pidetään aina ajan tasalla. Salassa pidettävää tietoa sisältäviin tehtäväluokkiin saa olla oikeudet vain sellaisilla käyttäjäryhmillä, joiden työtehtäviin kyseisten tietojen saatavuus kuuluu. Muilla ei saa olla mahdollisuutta nähdä salassa pidettävää tietoa tai salassa pidettäviä metatietoja. Käyttäjäryhmät määritellään TOS:iin joko tehtäväluokittain tai tehtäväkohtaisesti.

4 PILVIPALVELUMALLIT

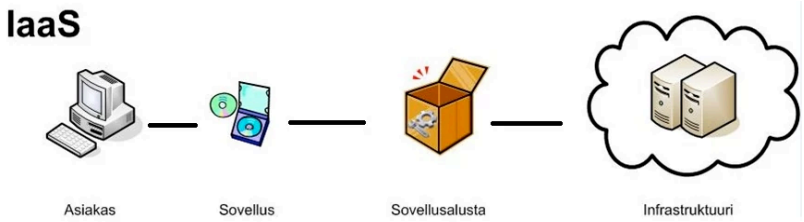
Pilvipalveluilla tarkoitetaan internetin kautta tarjottavia ohjelmistopalveluita ja tietoteknisiä resursseja. Pilvipalvelumallit jaetaan yleensä kolmeen erilaiseen pääkategoriaan: SAAS, IaaS ja PaaS.

SaaS (Software as a Service) eli ohjelmiston hankkiminen palveluna on normaalista ohjelmiston ostamisesta, asentamisesta ja ylläpidosta poiketen sovelluksen ostamista palveluna. Yritys maksaa silloin sovelluksesta esim. aikaperusteisen käyttäjä- tai konekohtaisen maksun. Tällöin pääoman sitominen ohjelmistoon ja/tai laitteistoon vähenee ja henkilöresursseja vapautuu yrityksen kannalta tuottavampiin tehtäviin (Kuva 7).



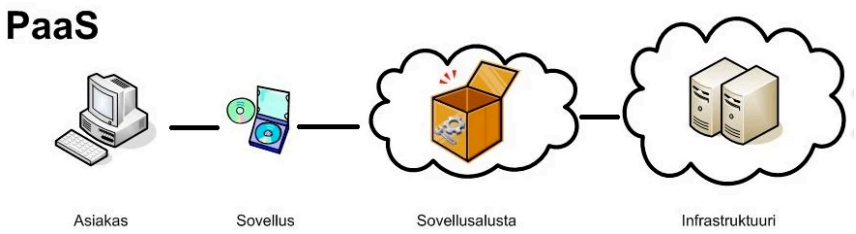
Kuva 7. SaaS-malli

IaaS (Infrastructure as a Service) eli infrastruktuurin ostaminen palveluna tarkoittaa laitteiston resurssien hankkimista palveluna. IaaS:n hyviksi puoliksi lasketaan joustavuus, resurssien yhteiskäyttö, itsepalvelu, automaatio ja käyttöön perustuva laskutus (Kuva 8).



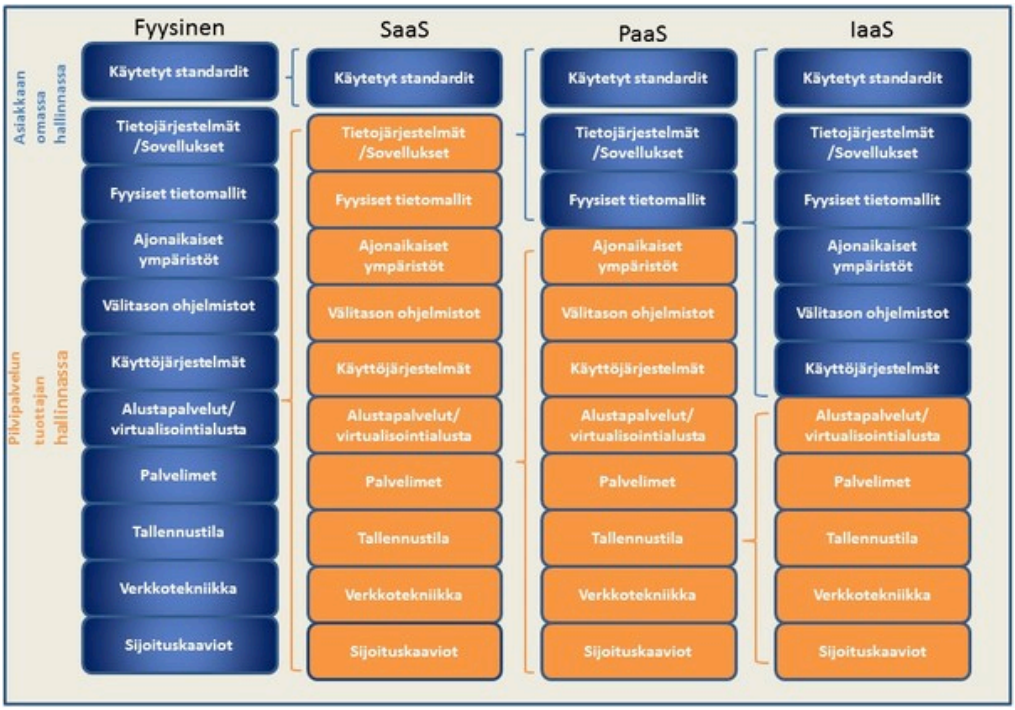
Kuva 8. IaaS-malli

PaaS (Platform as a Service) on edellä mainittujen mallien välimuoto, eli siihen kuuluvat palvelun hankkimisessa määritellyt teknologiapalvelut. Palvelualustat ovat virtualisoituja ja niiden ylläpito ja kehitys jää palvelun-tarjoajalle. Etuna pidetään joustavaa sovelluskehitystä, sovellusten testausta ja käyttöönottoa ilman laitteiston ja ohjelmistojen omistamista (Kuva 9) (Jhs-suositukset.fi 2017).



Kuva 9. PaaS-malli

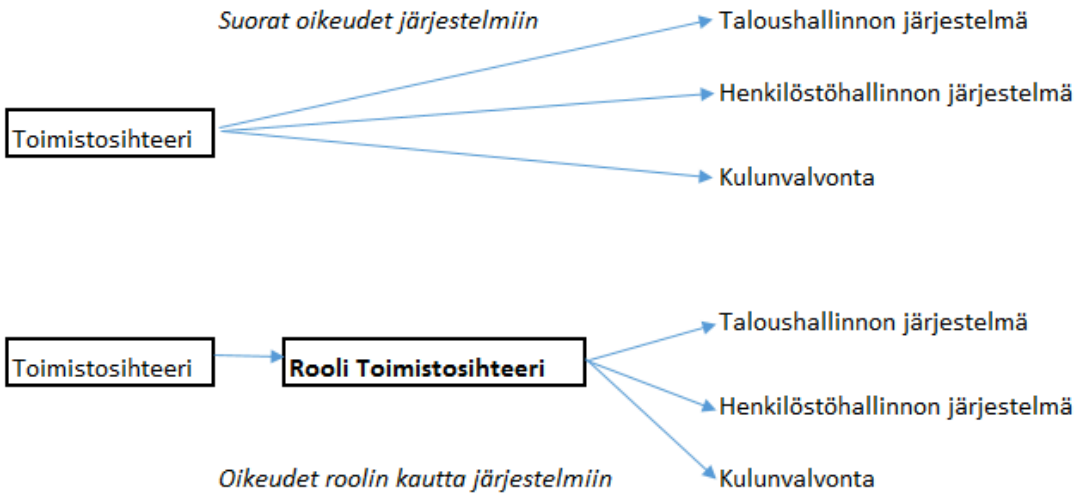
Alla olevassa kuvassa on havainnollistettu eri palvelumallien vastuujaot. Sinisellä värillä on merkitty kokonaisuudet, jotka ovat asiakkaan omassa hallinnassa ja oranssilla värillä pilvipalvelun tuottajan hallinnassa olevat kokonaisuudet (kuva 10).



Kuva 10. Pilvipalvelumallien vastuujaot (Jhs-suositukset.fi)

5 ROOLIPOHJAINEN KÄYTTÄJÄHALLINTA

Roolipohjaisessa käyttäjähallinnassa oikeuksia ei anneta suoraan henkilöille vaan rooleille. Roolit taas ovat joukko yksittäisiä käyttöoikeuksia, joita organisaation työntekijät tarvitsevat työssään. Työntekijät saavat siis oikeudet vain kun heidän sijoitetaan rooleihin (Kuva 11).



Kuva 11. Suorat oikeudet vs. roolipohjaisuus

Roolipohjaisen käyttäjähallinnan periaate perustuu siihen, että organisaation sisäiset roolit pysyvät suhteellisen samoina. Rooleja voidaan määritellä kahdella eri tavalla; Bottom-up tai Top-down. Bottom-up-menetelmässä tarkistetaan mitä erilaisia käyttöoikeuksia työntekijöillä on ja yritetään löytää yhteisiä nimittäjiä, joihin rooli voisi pohjautua. Vaikka tämä menetelmä on suhteellisen nopea ja helppo, tuloksena voi kuitenkin olla että käyttäjillä on liikaa oikeuksia. Top-down-menetelmässä taas mietitään mitä yhteisiä käyttäjäryhmiä pitäisi olla, joko työtehtäviin tai organisaatioon perustuvia ja määritellään roolit sen mukaan. Ko. menetelmä on hitaampi, mutta kauaskantoisempi ja vaatii tekijältään laajempaa tietoa organisaatiosta (Inno-vointi.fi 2016).

Järjestelmäpohjaisilla rooleilla tarkoitetaan järjestelmien sisäisten oikeuksien hallintaa roolien avulla. Roolin sisältämät oikeudet voivat olla esi-

merkiksi lukuoikeudet ohjelmaan, tietyt kirjoitusoikeudet ja oikeus tehdä tilauksia.

Toiminnallisella roolilla tarkoitetaan henkilön työtehtäviin, työyksikköön tai titteliin liittyviä rooleja, joilla kuvataan mitä oikeuksia työssä tarvitaan. Käyttöoikeudet voivat olla tietojärjestelmän rooleja, käyttäjäryhmiä tai oikeuksia fyysisiin käyttöoikeuksiin kuten kulkulupiin. Työrooleilla on mahdollista hallita koko organisaation kaikkia käyttöoikeuksia. Tehokkain tapa roolipohjaisessa käyttäjähallinnassa on käyttää näitä edellä mainittuja rooleja yhdessä.

Roolipohjaisella käyttäjähallinnalla tavoitellaan tietysti hallittavuutta. Käyttöoikeuksien antaminen suoraan henkilölle vie hallittavuutta sitä enemmän mitä isommasta organisaatiosta on kyse. Roolien kautta käyttöoikeuksien antaminen on myös nopeampaa sekä helpottaa oikeuksien poistamista henkilöiltä työsuhteen päättyessä.

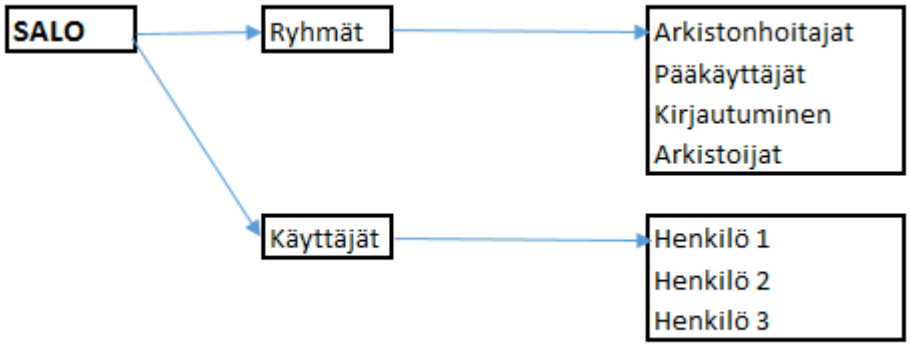
Roolien avulla pystytään henkilöiden käyttöoikeuksia myös rajaamaan ja estämään esimerkiksi käyttöoikeuksien vaarallisia yhdistelmiä. Roolit antavat myös mahdollisuuden raportointiin, jolla voidaan tarkistaa ovatko henkilöt käyttöoikeudet juuri ne, joita hän työssään tarvitsee. Hallintaa roolien kautta pidetään yleisesti tietoturvallisempana vaihtoehtona kuin yksittäisten oikeuksien antamista suoraan henkilöille.

Roolipohjaisessa käyttäjähallinnassa oikeudet määritellään yhdessä organisaation yksiköiden kanssa. Yksiköiden esimiehet tuntevat parhaiten oman yksikkönsä toiminnan ja pystyvät kertomaan miten oikeudet määritellään henkilöiden ja työtehtävien mukaan. Tietohallinnolle jää roolien määrittelyt järjestelmään, yksiköltä tulevien tietojen mukaan. Roolien suunnittelussa pyritään minimoimaan roolien määrä, jolloin myös hallittavuus säilyy. Roolit suunnitellaan niin että hyväksymisprosessi olisi mahdollisimman nopea.

6 SARKK JA KÄYTTÄJÄHALLINTA CASE SALO

SARKKia pilotoitiin Salon kaupungissa vuoden 2012 keväällä. Tavoitteena oli ottaa järjestelmä käyttöön parin vuoden sisällä mutta aikatauluista ja resursseista johtuen siihen ollaan vasta nyt pääsemässä. Samalla kun järjestelmää on rakennettu, on huomattu tarve tarkemmalle käyttäjähallinnalle kuin mitä järjestelmän toimittaja tarjoaa. Salaisia tehtäväluokkia on tällä hetkellä noin 170 kpl. Kyseiset tehtäväluokat sisältävät henkilötietoja tai muita salassa pidettäviä tietoja, joille pääsy pitää rajata. Kaikkiaan tehtäväluokkia on noin 900, mutta tässä tutkimuksessa keskitytään salaisten tehtäväluokkien rajaamiseen.

Järjestelmän toimittajalla on valmiina Active Directory-ympäristö, jolla ylläpidetään oikeuksia viiteen eri ryhmään: pääkäyttäjät, arkistonhoitajat, arkistoijat, kirjautumisoikeudet (kirjautuminen) ja kaikki käyttäjät (julkiset asiakirjat). Kyseisillä ryhmäoikeuksilla saa kaikkeen sähköisesti arkistoivaan tietoon oikeudet. Eli jos kuuluu ryhmään arkistoija, saa arkistoida kaikkiin tehtäväluokkiin asiakirjoja. Nämä ryhmäjäsenyydet eivät erottele eri tehtäväluokkia, vain julkiset tehtäväluokat ovat nähtävissä, mutta salaisiin tehtäväluokkiin voivat arkistoijat arkistoida vaikka eivät näe asiakirjoja tai metatietoja jälkeenpäin. AD:ssa myös kansiorakenne oli yksinkertainen, ryhmät ja käyttäjät oli jaettu eri kansioihin (Kuva 12).



Kuva 12. Lähtötilanne järjestelmän toimittajan palvelimella

Koska tavoitteena on saada selkeä työroolin mukainen rajaus oikeuksiin, pitää koko organisaatiota tarkastella isommassa mittakaavassa, ei vain yksittäisiä yksiköitä. Eli mihin voi perustua käyttäjähallinta, kun eri yksi-

köiden/osastojen tehtävät ovat kuitenkin toisista poikkeavia. Tosin samankaltaisuuksiakin yksiköiden välillä on. Esimerkiksi jokaisessa yksikössä on esimies ja hyvin usein myös toimistosihteeri. Näiden työroolit ovat useimmiten yksiköiden välillä yhteneväiset. Entä onko jokaisessa yksikössä arkistoitavia asiakirjoja ja onko yksiköiden työntekijöiden välillä erilaisia rooleja. Tarvitseeko jokaisen yksikön työntekijän päästä katsomaan samoja tietoja vai ovatko oikeudet henkilökohtaisia vai yksikkökohtaisia.

Tavoitteena on rakentaa SARKKiin joustava, helppokäyttöinen ja pitkäikäinen roolipohjainen käyttäjähallinta, joka palvelee mahdollisimman pitkäikäisesti muuttuvassa organisaatiossa. Tutkimuksessa keskitytään salaisiin tehtäväluokkiin, muut tehtäväluokat voidaan rakentaa samalla tavalla myöhemmin. Käyttäjähallinta rakennetaan toimittajan palvelimelle ja sitä tulee jatkossa käyttämään hallintopalveluissa sähköisestä arkistoinnista vastaava henkilö.

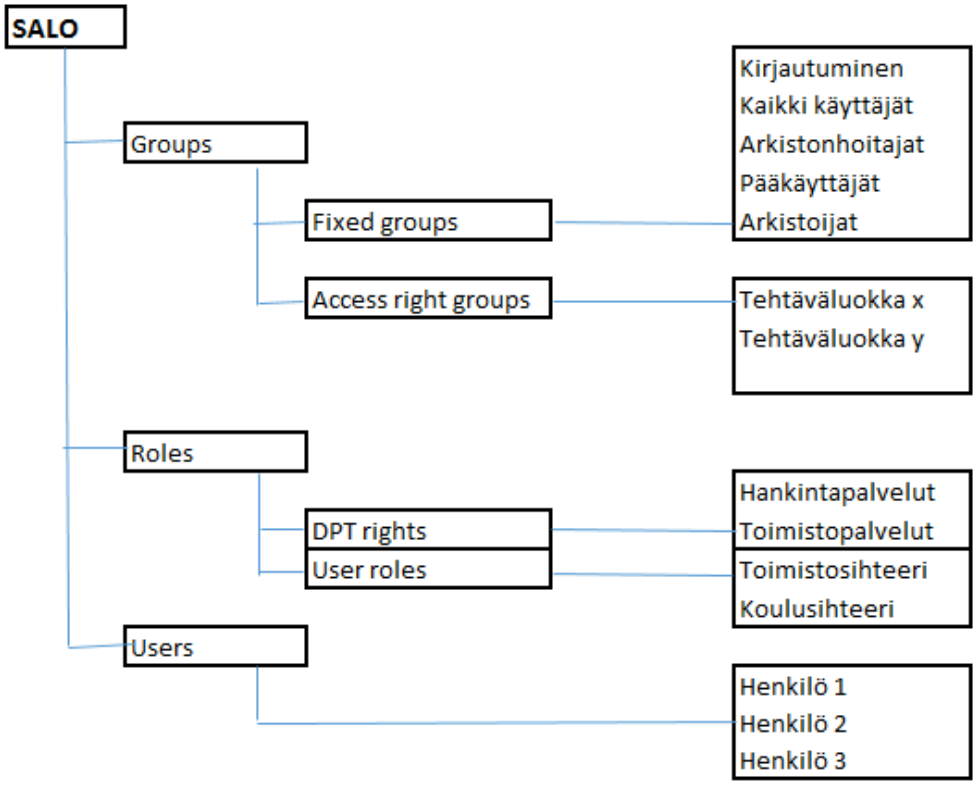
On useita vaihtoehtoja rakentaa käyttäjähallinta. Tärkeintä alkuvaiheessa on miettiä, mikä toimii organisaatiossa ja järjestelmässä parhaiten ja mahdollisimman vähällä ylläpidolla. Vaikka työ alussa vaatisikin paljon aikaa ja resursseja, palkitsee se myöhemmin hallittavuudella.

SARKKin käyttäjähallinnan salaiset tehtäväluokat vaativat eniten työtä ja tämän tutkimuksen tekoaikana TOJ:ssa on niitä n. 170 kpl. Päätehtävät, joita on Salossa 14 kpl, sisältävät useita alatehtäviä ja ne taas tehtäviä, ja kaikissa tasoissa voi olla salaisia luokkia. Ylläpitäjällä pitää siis olla tarkasti tiedossa ko. tehtäväluokat ja kenellä mihinkin tehtäväluokkaan on työn puolesta oikeus päästä katsomaan. Lisäksi tulevat tehtäväluokat joihin työnkuvan perusteella saadaan arkistoida. Kumpikin oikeus, sekä arkistointi tehtäväluokkaan ja tehtäväluokan katseluoikeus, annetaan erillisinä. Käyttäjähallintaa voitaisiin tietysti jatkaa toimittajan tavalla, oikeuden perustuessa yleisoikeuksiin. Silloin jokainen tunnuksen SARKKiin saanut pääsisi katsomaan ja arkistoimaan jokaiseen tehtäväluokkaan.

Koska tavoite on hallittavassa käyttäjähallinnassa, roolien määrittelyssä ja tietoturvallisessa ympäristössä, lähdin käyttäjähallinnan määrittelyssä liikkeelle top-down-menetelmällä. Tutkimalla TOS-prosesseja ja organisaatiota sain hahmotettua käyttäjähallinnan tarpeen ja mittakaavan. Jo tässä vaiheessa huomattiin että ihan täysin toimivaa yhtä tapaa tehdä SARKKin käyttäjähallintaa ei ole. Pitkälti TOS-prosessit ovat palvelualuekohtaisia ja palvelualueiden määrittelemiä, mutta yli yksikkörajojen tarvitaan myös oikeuksia. Vastuu prosesseista ja niiden määrittelystä on aina yksiköillä. Tarvitaan siis työnkuvaan/työtehtävään perustuvia rooleja mutta myös yksikköön ja toimialoihin perustuvia rooleja. Roolien määrittelyssä tulee ottaa huomioon, miten paljon organisaation muuttuessa tarvitaan työtä, että käyttäjähallinta saadaan ajan tasalle. Silloin pitää SARKKin käyttäjähallinnan pystyä vastaamaan tarpeeseen.

6.1 Perusoikeudet

Koska jokaisella työntekijällä on oikeus päästä katsomaan julkisia asiakirjoja, pitää järjestelmään olla ns. perusoikeus, rooli nimeltään kaikki käyttäjät. Lisäksi tarvitaan pääkäyttäjäoikeudet, joilla on kaikki oikeudet kaikkiin tehtäväluokkiin. Arkistoijat (60 henkilöä), jotka ovat yksikkökohtaisia ja arkistonhoitajat (5 henkilöä) oikeuden saavat ne henkilöt, joiden työnkuvaan ko. työt kuuluvat. Ohjelmiston toimittajan määrittelemät ryhmät ja tehtäväluokkakohtaiset ryhmät jäävät AD:ssa Salo-kansion alle nimeltä Groups. Rooleille tehdään oma kansio Roles, johon sijoitetaan kaikki roolit, niin yksikkö- kuin työnkuvaan perustuvat roolit. SARKKiin määritellään käyttäjiä/tunnuksia aina tarpeen mukaan. Nämä käyttäjät perustetaan omaan kansioon Users. Kansiorakenteen selventämiseksi jaetaan vielä Groups-ryhmäoikeudet Fixed groups-ryhmään, jossa toimittajan määrittelemät ryhmät ja Access rights groups-ryhmään, jossa salaiset tehtäväluokkakohtaiset oikeudet ovat. Roolit jaetaan kahteen ryhmään, yksikkökohtaisiin- ja työnkuvaan perustuviin rooleihin (Kuva 13). Näin saadaan selkeämpi ja hallittavampi kokonaisuus käyttäjähallinnan ylläpitoon. Käytännössä kun uusi tunnus tehdään järjestelmään, oikeudet annetaan users-ryhmässä henkilölle add to group–toiminnolla.

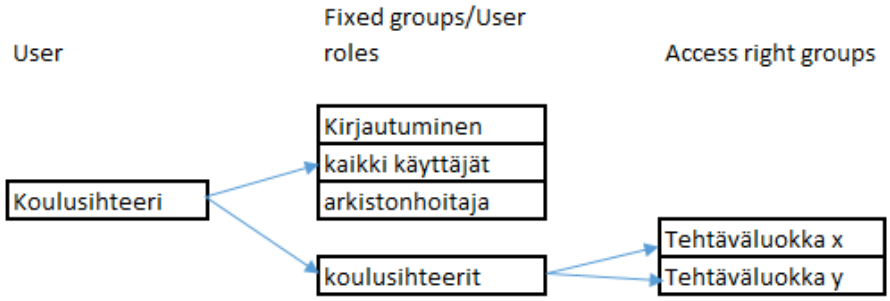


Kuva 13. Uusi AD-rakenne

6.2 Roolien rakentaminen

Paras hallittavuus roolipohjaisella käyttäjähallinnalla saavutetaan yhdistelemällä järjestelmäpohjaisia- ja toiminnallisia rooleja. SARKK:in käyttäjähallintaa varten tarvitaan sekä yksikköön että työnkuvaan perustuvia rooleja, joista kaikki perustuvat henkilön asemaan organisaatiossa. SARKKin sisällä taas käsitellään järjestelmäpohjaisia rooleja, kun tehtäväluokkakohtaisia oikeuksia sijoitetaan eri rooleihin.

Käytännössä *työnkuvaan perustuvan roolin* rakentaminen aloitetaan lisäämällä henkilö kirjautuminen- ja kaikki käyttäjät-ryhmään. Esimerkiksi jokaisessa koulussa koulusihteeri kuuluu arkistonhoitajat-ryhmään ja sen lisäksi hänen pitää päästä katsomaan useampaa salaiseksi luokitellun tehtäväluokan asioita. Tehdään rooli koulusihteerit, johon lisätään yksittäisiä pääluokan 12 tehtäväluokkia. Koulujen koulusihteerit kuuluvat siis ryhmiin kaikki käyttäjät, kirjautuminen, arkistonhoitajat ja koulusihteerit (Kuva 14).



Kuva 14. Koulusihteerin oikeudet

Yksikkökohtaisia rooleja tarvitaan kun yksikön työntekijät tarvitsevat pääsyn oman toimialueensa salaisiksi luokiteltuihin asioihin. Tällöin esimerkiksi hankintapalveluiden henkilöt kuuluvat ryhmiin kaikki käyttäjät, kirjautuminen ja hankintapalvelut–ryhmään, joka sisältää ne tehtäväluokat joissa on salaiset asiat. Kuvan 10 rakenne toistuu myös yksikkökohtaisissa rooleissa. Organisaatiossa on tietysti rooleja, jotka voivat olla vain yhdellä henkilöllä, esim. hallintojohtaja. Tällöin rooleista tulee asemaan perustuvia ja vain yhdellä henkilöllä on tämä oikeus. Kun tulee tilanne että tällaista yhden henkilön roolia pitää sijaistaa, voidaan tehdä uusi rooli hallintojohtajan sijainen, koska oikeudet sijaisilla eivät välttämättä ole aivan samat.

Tarvetta *erikoisrooleille* ei koettu tässä vaiheessa tärkeiksi. Mikäli organisaatioon tulisi esimerkiksi projektityöntekijä, lähdettäisiin siitä että yksikkökohtaiset oikeudet olisivat riittävät. Mikäli erikoisroolia tarvittaisiin

esim. tukitoimintojen projektityöntekijälle, pitäisi rooli koota erikseen tehtäväluokka kerrallaan. Myös ulkopuolisille toimijoille voidaan antaa oikeudet SARKK:in käyttöön, silloin oikeus annetaan ryhmään kirjautuminen ja lisäksi yksittäiset tehtäväluokat käyttötarkoituksen mukaan.

6.3 Muutostilanteet

Tällaisten roolien toimiva käyttö perustuu tietysti organisaatiorakenteen suhteelliseen vakaaseen tilaan. Muutostilanteet tuovat aina haasteita käyttäjähallinnan ylläpitäjälle ja seuraavaksi mietitäänkin miten käytännössä järjestelmä tässä joustaa.

Oikeudet annetaan aina henkilölle (User) lisäämällä Fixed groups- ja user roles-oikeudet. Henkilömuutos ei siis muuta rooleja, koska rooli ei perustu henkilöön vaan henkilön työnkuvaan organisaatiossa. Jos rooleihin liittyvät tehtäväluokat muuttuvat tehdään muutos suoraan rooliin (User role) muokkaamalla tehtäväluokkakohtaisia oikeuksia esim. tehtäväluokan vaihto tai lisäys. Nimikemuutokset organisaatiossa aiheuttavat myös SARKK:in käyttäjähallinnan rooleissa (User role) muutoksen, koska ne perustuvat työnkuvaan/titteliin. Ko. muutos ei kuitenkaan ole isotöinen.

Organisaatiorakenteen muutos taas aiheuttaa enemmän työtä käyttäjähallintaan, koska se muuttaa myös TOJ:n rakennetta esim. yksikön siirtyessä toisen päätehtäväluokan alle. Silloin muuttuu myös käyttäjähallinnassa oikeudet uusien tehtäväluokkanumeroiden muodostuessa. Vanha tehtäväluokka lopetetaan ja kun uusi eri numerolla oleva tehtäväluokka perustetaan, rooliin (User role) lisätään uuden tehtäväluokan numero. Vanha jää voimaan, jolloin vanhan tehtäväluokan oikeus säilyy ennallaan ja ko. luokan asiakirjoja pääsee vielä katsomaan. Yhdellä henkilöllä voi olla myös useita rooleja, jolloin henkilölle lisätään useampi rooli (User role).

7 Yhteenveto

Tätä opinnäytetyötä lähdin tekemään aiheesta, josta minulla ei ollut ennakkoon selkeää tietoa, vaikka ko. aiheen pitäisi koskettaa jokaista kaupungin työntekijää jollain tasolla. Teoriaosiota kirjoittaessa hahmottui arkistoinnin ja asiahallinnan tarkoitus ja merkitys organisaatiossa, luin useita artikkeleita asiaan liittyen. Hankalaa oli tuoda asiaa esille selkeästi ja tiivistetysti, tietoa löytyi melkoisesti. Sähköinen arkistointi taas oli selvästi vaikeampi osuus, tähän ollaan vasta siirtymässä ja siirtymäajatkin ovat kovin pitkiä. Selkeää infoa ei aiheesta löytynyt, enemmänkin hajanaisia artikkeleita.

SARKK:iin ei ole tämän tutkimuksen aikana vielä tehty omaa tehtäväluokkiin perustuvaa käyttäjähallintaa Saloa lukuun ottamatta. Tuoteperheen SARKK-osio on käytössä vain Salossa mutta tuoteperheen muita osioita on käytössä muissa kunnissa. Salossa SARKK:lle kuitenkin oli selkeä tarve; tietoturva ja hallittavuus koettiin tärkeiksi.

Isoin työ roolipohjaisen käyttäjähallinnan rakentamisessa on roolien löytäminen ja määrittely. Isossa organisaatiossa roolien määrittelyyn tarvitaan aina yksiköiden apua, vaikka järjestelmän toiminnot olisivat ylläpitäjälle hyvinkin selkeät. Muutostilanteet tuovat ylläpitäjälle aina töitä joten olisi hyvä että korkeamman tason tehtäväluokat voisi lukita pysyviksi, jolloin muutoksien mahdollisuus vähenisi ja käyttäjähallinnan hallittavuus paranisi.

Salon kaupungissa on käytössä IDM-järjestelmä (Identity manager l. identiteetin hallintajärjestelmä), jonka avulla SARKK:in oikeudet olisi mahdollista saada automatisoitua yhden liittymän kautta. Tämä tietysti vaatisi oikeutta päästä viemään oikeudet suoraan toimittajan palvelimelle. Toistaiseksi oikeudet haetaan IDM:ssä, jossa esimiehen hyväksynnän jälkeen pyyntö siirtyy SARKK:in käyttäjähallinnasta vastaavalle, joka lisää oikeudet järjestelmään.

SARKK:iin on myös mahdollista saada kuntalaisten käyttöön oma käyttöliittymä, jolla kaupungin asukkaat pääsisivät tunnistautumisen kautta katsomaan julkisia asiakirjoja. Toistaiseksi tietoturvaseikat ovat estäneet kyseisen osan käyttöönoton.

LÄHTEET

Arkisto.fi 2017
Viitattu 2.10.2017
https://www.arkisto.fi/fi/viranomaisille-2/Julkishallinnon-asiakirjahallinnon-ja-arkistotoimen-ohjaus#ohjeet

Fujitsu 2012
Viitattu 30.3.2017
http://www.fujitsu.com/fi/about/resources/news/pressreleases/2012/sarkk_palvelu.html

Inno-vointi.fi 2016
Viitattu 28.5.2017
http://www.inno-vointi.fi/fi/innovoinnin-periaatteet/viitekehys-kaksi-lahestymistapaa

Jhs-suositukset .fi 2017
Viitattu 2.10.2017
http://docs.jhs-suositukset.fi/jhs-suositukset/JHS179_liite9/JHS179_liite9.html

Kunnat.net 2016
Viitattu 14.4.2017
Kuntaliiton verkkokauppa; Kuntasektorin asianhallinnan viitearkkitehtuuri ebook
http://shop.kunnat.net/product_details.php?p=3186

Kuntaliitto.fi 2002
Viitattu 3.10.2017
Kuntaliiton verkkokauppa; Kunnalllisten asiakirjojen säilytysajat
http://shop.kunnat.net/product_details.php?p=294

Kuntaliitto.fi 2017
Viitattu 3.10.2017
https://www.kuntaliitto.fi/asiantuntijapalvelut/tietoyhteiskunta/tiedonhallinta

Kansallisarkisto 2016
Viitattu 18.2.2017
http://www.arkisto.fi/fi/palvelut/julkisen-hallinnon-saehkoeiset-palvelut/saehke2-sertifiointi

Kansallisarkisto2008

Viitattu 21.2.2017
http://www.arkisto.fi/uploads/normit/valtionhallinto/maarayksetjaohjeet/normiteksti_suomi.pdf

Tietosuoja.fi 2017
Viitattu 4.10.2017
http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

Vtv.fi 2014
Viitattu 16.4.2017
https://www.vtv.fi/files/4161/11_2014_Sahkoisen_arkistoinnin_edistaminen.pdf