Juha Salmi

PERUSTIETOTEKNIIKAN PALVELUVERKKO
CASE: SATAKUNNAN SAIRAANHOITOPIIRI

Tietojenkäsittelyn koulutusohjelma
2009

PERUSTIETOTEKNIIKAN PALVELUVERKKO

CASE: SATAKUNNAN SAIRAANHOITOPIIRI

Salmi, Juha
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Tammikuu 2009
Grönholm, Jukka
UDK: 004.7
Sivumäärä: 41

Avainsanat: atk, palvelimet, järjestelmäarkkitehtuuri, pääsynvalvonta

Tämän opinnäytetyön aiheena selvitettiin ratkaisumalleja olemassaolevan suuren organisaation perustietotekniikka-infrastruktuurin päivittämiseksi. Opinnäytetyö sisältää perustason kuvauksen perustettavan Palveluverkon rakenteesta ja sen tärkeimpien palveluiden, kuten hakemistoratkaisun toteutuksesta.

BASIC INFORMATION TECHNOLOGY INFRASTRUCTURE SERVICES NETWORK
CASE SATAKUNNAN SAIRAANHOITOPIIRI

Salmi, Juha
Satakunta University of Applied Sciences
Degree in Business Information Technology
January 2009
Grönholm, Jukka
UDK: 004.7
Number of pages: 41

Key words: information technology, servers, system architecture, access control

The purpose of this thesis was to explore solutions to update basic information technology infrastructure of a existing large scale public enterprise. Thesis incluedes a brief description of a basic information technology infrastructure services network. Description of vital network services such as Directory Services is also included.

SISÄLLYS

1 TAUSTAA

Palveluverkko-hankkeen käynnistyminen on osa valtakunnallista Terveydenhuollon toimintojen muutosta. Palveluverkko on Satakunnan sairaanhoitopiirin tietotekninen vastaus tuleviin muutoksiin ja palvelurakenteen uudistamiseen. Käytössä olevat järjestelmät ja menetelmät ovat vanhentuneita, eivätkä ne vastaa tulevaisuuden tarpeisiin. Organisaatiomuutokset monimutkaistavat jo ennestään hankalasti hallittavaa tietojärjestelmäkokonaisuutta ja korostavat vanhentuneiden ratkaisuiden ongelmakohtia.

1.1 Sairaanhoitopiirijärjestelmä

Erikoissairaanhoitolaissa Suomi jaetaan 20:een Sairaanhoitopiiriin, joiden vastuulla on erikoissairaanhoidon ja siihen liittyvän toiminnan järjestäminen. Kullakin sairaanhoitopiirillä on oma perussopimus, joka määrittelee sairaanhoitopiirin toimintamallin. Erikoissairaanhoitolain mukaan jokainen kunta on velvoitettu kuulumaan johonkin Sairaanhoitopiiriin.
(Finlex, 2008)

Edellä mainitun lisäksi Suomi on jaettu paitsi sairaanhoitopiireihin, myös erityisvastuualueisiin erityistason sairaanhoidon järjestämistä varten. "Kuhunkin erityisvastuualueeseen kuuluu sellainen sairaanhoitopiiri, jonka alueella on lääkärikoulutusta antava yliopisto." Erityisvastuualueista ja siihen kuuluvista sairaanhoitopiireistä päättää Valtioneuvosto.
(Finlex, 2008)

1.2 Satakunnan sairaanhoitopiirin kuntayhtymä

Satakunnan sairaanhoitopiirin kuntayhtymä (jäljempänä Satakunnan sairaanhoitopiiri tai SATSHP) on Satakunnan alueen erikoissairaanhoidon toimintoja järjestävä toimija. Kuntayhtymällä on 24 jäsenkuntaa ja kuntayhtymä tarjoaa palveluita noin 226 000 asukkaalle yhteistyössä perusterveydenhuollon ja sosiaalitoimen kanssa. Satakunnan Sairaanhoitopiirin palveluksessa työskentelee noin 3 500 henkilöä. (SATSHP, 2008)

Satakunnan Sairaanhoitopiirin kuntayhtymä ja Varsinais-Suomen Sairaanhoitopiirin kuntayhtymä muodostavat erityisvastuualueen. Lääkärikoulutusta antavana yliopistona erityisvastuualueella on Turun yliopisto.
(Finlex, 2008)

1.3 Erikoissairaanhoitolain 10 §:n muutos

Erikoissairaanhoitolain 10 §:n muutos astui voimaan 17.9.2004. Lainkohdassa määritellään sairaanhoitopiirien tehtävät seuraavasti:

> Sairaanhoitopiirin kuntayhtymä vastaa alueellaan tässä laissa säädetyn erikoissairaanhoidon järjestämisestä yhtenäisin lääketieteellisin ja hammaslääketieteellisin perustein.
>
> Sairaanhoitopiirin kuntayhtymän tulee alueellaan huolehtia erikoissairaanhoitopalvelujen yhteensovittamisesta ja yhteistyössä terveyskeskusten kanssa suunnitella ja kehittää erikoissairaanhoitoa siten, että kansanterveystyö ja erikoissairaanhoito muodostavat toiminnallisen kokonaisuuden. Lisäksi sairaanhoitopiirin kuntayhtymän tulee sille kuuluvia tehtäviä hoitaessaan olla alueensa kuntien sosiaalitoimen kanssa sellaisessa yhteistyössä, jota tehtävien asianmukainen suorittaminen edellyttää.
>
> Sairaanhoitopiirin kuntayhtymän tulee antaa alueensa terveyskeskuksille niiden tarvitsemia sellaisia erikoissairaanhoidon palveluja, joita terveyskeskusten ei ole tarkoituksenmukaista tuottaa sekä vastata terveyskeskusten tuottamien laboratorio- ja kuvantamispalvelujen, lääkinnällisen kuntoutuksen sekä muiden vastaavien erityispalvelujen kehittämisen ohjauksesta ja laadun valvonnasta.

> Lisäksi sairaanhoitopiirin kuntayhtymän tulee alueellaan huolehtia tehtäväalaansa kohdistuvasta tutkimus-, kehittämis- ja koulutustoiminnasta sekä tietojärjestelmien yhteensovittamisesta. Kuntayhtymän tulee myös huolehtia siitä, että terveydenhuollon henkilöstö peruskoulutuksen pituudesta, työn vaativuudesta ja toimenkuvasta riippuen osallistuu riittävästi heille järjestettyyn täydennyskoulutukseen. Sosiaali- ja terveysministeriö voi antaa tarvittaessa tarkemmat säännökset täydennyskoulutuksen sisällöstä, laadusta, määrästä, järjestämisestä, seurannasta ja arvioinnista.
> (Finlex, 2008)

Satakunnan Sairaanhoitopiirissä on huomioitu lakimuutoksen asettaman velvollisuuden liittyen alueen terveyskeskuksille tarjottavista erikoissairaanhoidon palveluista sekä tietojärjestelmien yhteensovittamisesta. Käytännössä lakimuutos on käynnistänyt prosessit Satakunnan Sairaanhoitopiirin Sairaanhoidolliset palvelut -tulosalueen liikelaitostamiseksi, Alueellisen tietohallintosuunnitelman luomiseksi sekä Tietopalvelut-yksikön palvelutuotannon uudelleenorganisoimiseksi.
(Tietopalvelut-yksikön johtoryhmä, 2006, Tietopalvelut-yksikön johtoryhmä, 2007)

1.4 Satakunnan erityishuoltopiirin kuntayhtymä

Sairaanhoitopiirijärjestelmän rinnalla Suomessa toimii Erityishuoltopiirijärjestelmä, jonka tehtävänä on järjestää palveluita kehitysvammaisille. Satakunnan alueella palvelua järjestää Satakunnan erityishuoltopiirin ky. Helmikuussa 2007 voimaantulleen kunta- ja palvelurakenneuudistusta koskevan lain 6 §:n muutoksen johdosta Satakunnan Erityishuoltopiiri ja Satakunnan Sairaanhoitopiiri aloittivat yhteistyöneuvottelut. Kevään 2008 neuvottelujen tuloksena päätettiin Satakunnan Erityishuoltopiirin liitoksesta Satakunnan Sairaanhoitopiiriin 1.1.2009 alkaen.

Tietohallinnon toimintojen kannalta muutos tarkoittaa koko Satakunnan Erityishuoltopiirin IT-järjestelmien ja laitteistojen vaiheittaista liittämistä Palveluverkkoon. Muutosprosessista ja järjestelmälinjauksista sovitaan erikseen organisaatioiden välisellä sopimuksella. Sopimuksen mukaan vuoden 2008 lopussa toteutetaan vain välttämättömät muutokset ja vuosi 2009 varataan järjestelmälinjausten tekemiseen ja muutosten suunnitteluun. Muutokset käynnistetään vuoden 2010 alussa.

1.5 Alueellinen tietohallintosuunnitelma

Erikoissairaanhoitolain 10 §:n muutoksen tultua voimaan Satakunnan sairaanhoitopiirissä käynnistettiin yhteistyössä Satakunnan kuntien ja kuntayhtymien kanssa Alueellisen tietohallintosuunnitelman laadinta. Suunnitelman tarkoitus oli kartoittaa Satakunnan terveydenhuollon organisaatioiden IT-yksiköiden ja -toimijoiden tilannetta ja laatia kehittämispolku. Suunnitelma tehtiin työryhmätyöskentelynä ja kyselytutkimuksella.

Työryhmätyöskentelyn ja kyselytutkimuksen mukaan terveydenhuollon toimijoiden ongelmat ovat seuraavat:

- Tietohallinnon organisointi ja ohjausmekanismit

- Organisaatiolähtöisyys

- Tietojärjestelmien standroimattomuus

Parhaaksi ratkaisuksi ongelmiin todettiin toimijoiden välisen yhteistyön tiivistäminen ja alueellisen toimijan perustaminen. Vertailukohtana on käytetty Varsinais-Suomen Sairaanhoitopiirin alueella toimivaan tietohallintoyksiköiden neuvottelukuntaa, jossa jäseninä ovat kaikki alueen toimijat. Neuvottelukunnassa sovitaan yhteisistä kehittämishankkeista. Varsinais-Suomen Sairaanhoitopiirin alueelle on perustettu alueelliseksi toimijaksi osakeyhtiö, jonka tehtävänä on tuottaa IT-palveluita omistajilleen. (Alueellinen tietohallintosuunnitelma, 2006)

1.6 Kansalliset järjestelmät

Siirtyminen potilastietojen sähköiseen arkistointiin ja välittämiseen edellyttää yksittäisten tai alueellisten järjestelmäkokonaisuuksien lisäksi valtakunnallisia hakemistoja ja tietosäiliöitä. Satakunnan Sairaanhoitopiirin ja Varsinais-Suomen Sairaanhoitopiirn alueella käytössä oleva Fujitsun toimittama Fiale-aluetietojärjestelmä on askel kohti kansallisia järjestelmiä. Fiale-järjestelmä on viitetietokanta, jonka viitesisältö generoidaan eräajoina organisaatioiden perusjärjestelmistä. Tieto säilyy perusjärjestelmissä, mutta ne voidaan katselua varten ladata viitteiden osoittamasta paikasta. Fiale-järjestelmässä tietojen vaihto on organisaatiotasolla kaksisuuntaista: perusterveydenhuollon käytettävissä ovat omien tietojen lisäksi erikoissairaanhoidon tiedot ja erikoissairaanohoidolla vastaavasti perusterveydenhuollon tiedot. Tavoitteena on saada kaikki syntyvä potilastieto katseltavaksi Fiale-järjestelmän kautta. Käyttäjien tunnistamiseen käytetään toimikorttia ja sairaanohoitopiirien varmennepalvelua.

Kehitteillä olevat kansalliset järjestelmät eroavat Fiale-järjestelmästä siten, että varsinaiset tiedot keskitetään kansallisten järjestelmien tietokantoihin. Rakenne ei ole viitepohjainen, vaan organisaatioiden perusjärjestelmät tuottavat sisällön suoraan kansallisten järjestelmien tietosäiliöihin. Kansallisten järjestelmien järjestämisvastuuseen valittin Kansaneläkelaitos. Ensimmäisenä osana käyttöön on tulossa sähköinen reseptitietojärjestelmä, eResepti, jota käyttävät myös julkisen terveydenhuollon lisäksi yksityiset apteekit.

1.7 Nykytilan kuvaus

Nykyiset käytössä olevat tietojärjestelmät on rakennettu siten, että niiden tarkoituksena on tuottaa palveluita vain omistajaorganisaatiolle. Vanhimmat käytössä olevat järjestelmät on rakennettu 1980-luvun lopulla ja toimivat osittain vielä alkuperäisellä laitealustalla. Järjestelmien tekninen osaaminen on heikkoa niissä käytettyjen aikanaan edistyksellisten mutta nykypäivänä marginaalijärjestelmien vuoksi. Siirtyminen

palvelutuotantomalliin on haasteellinen prosessi, erityisesti operatiivisten sovellusten osalta, joihin ei alun perin ole sisäänrakennettu moniorganisaatiomallin mukaisen toiminnan rakenteita. Tällä tarkoitetaan tarkoitetaan järjestelmää, jossa tieto tallennetaan yhteen ja samaan tietovarastoon, mutta sen käsittelyssä ja näkyvyydessä on otettu huomioon tiedon omistaja- ja suojausmääritteet. Tiedon suojaus ja näkyvyyden rajoittaminen on erityisen tärkeää terveydenhuollon toimialalla, jossa tietojen käsittelyä rajoittaa laki rekisterin pitäjyydestä ja terveydentilaa koskevien tietojen luovuttamisesta.
(Alueellinen tietohallintosuunnitelma, 2006)

Satakunnan Sairaanhoitopiirin nykyiset tietotekniikkapalvelut tuottaa Tietopalvelut-yksikkö, jossa työskentelee noin 30 henkilöä. Yksikön toiminta jakaantuu kahteen osaan, käyttö- ja tukipalveluttiimiin sekä kehittämis- ja ylläpitotiimiin. Yksinkertaistettuna käyttö- ja tukipalvelutiimin tehtävänä on perustietotekniikasta huolehtiminen ja kehittämis- ja ylläpitotiimi vastaa operatiivisten sovellusten toiminnasta. Tietopalvelut-yksikkö tuottaa myös asiantuntijapalveluita Satakunnan ja Varsinais-Suomen alueen terveydenhuollon toimijoille.

Alueellisen tietohallintosuunnitelman valmistelun yhteydessä tehdyn tutkimuksen mukaan alueen toimijoiden tietotekniikkapalvelut on järjestetty monella eri tavalla. Osa organisaatioista hankkii kaiken ostopalveluna, osa hoitaa omana työnä tai näiden sekoituksena. Pienimmillä organisaatioilla nimettyä tietohallintohenkilökuntaa ei tutkimuksen mukaan ollut lainkaan. Lisäksi tietohallintosuunnitelman tutkimuksessa selvisi, että Satakunnan alueen terveydenhuollon organisaatioiden käytössä yli 200 eri ohjelmistoa. Pääsääntöisesti ostopalvelun kohteena oli perustietotekniikka, ei niinkään tietohallinnon toiminnot.

Tietohallinnon näkökulmasta järjestelmien nykytila ja tulevaisuuden haasteet luovat yhtälön, johon ei ole yksinkertaista ja helppoa ratkaisua. Alueellisen tietohallintosuunnitelman mukaan tietojärjestelmiä pitäisi kehittää kokonaisuutena, sekä perustietotekniikan ja operatiivisten järjestelmien muuntautumiskyky huomioiden. Organisaatioiden tiukkenevat resurssit eivät mahdollista aloittamista tyhjältä pöydältä. Erityisen hankalaksi koettiin suurien järjestelmähankkeiden vaiheistus: jotta operatiivisen sovelluksen perustietotekniikkavaateet voitaisin täyttää, pitäisi tarvittavien lait-

teisto- ja ohjelmistotarpeiden olla tiedossa mahdollisimman aikaisin. Jo pelkästään Satakunnan Sairaanhoitopiirin 2500 työaseman vaihtaminen tai päivittäminen kerralla uuteen on käytettävissä olevin resurssein mahdotonta. Muutokset on tehtävä vaiheittan, huolehtien loppukäyttäjien koulutuksesta ja järjestelmien käytön katkottomuudesta.

1.7.1 Perustietotekniikka

Perustietoteniikka-käsitteellä tarkoitetaan Palveluverkossa kaikkia niitä järjestelmiä ja laitteistoja, joita tarvitaan operatiivisten sovellusten käytön mahdollistamiseksi:

- työasemalaite, ohjauslaitteet, näyttölaite
- tulostinlaitteet
- työaseman käyttöjärjestelmäohjelmisto laiteajureineen
- toimisto-ohjelmapaketti, varus- ja apuohjelmat
- verkon peruspalvelut ja niiden tuottamiseen tarvittavat palvelinlaitteet
- tietoliikenneverkko ja verkon aktiivilaitteet
- työaseman, verkon peruspalveluiden ja tietoliikenneverkon hallinta
- käytettävien järjestelmien ja laitteiden tukipalvelu
- tunnistautumisvälineet, käyttäjän tietojen hallinta

Perustietotekniikan ajantasaisuus ja kokonaisvaltainen hallinta todettiin olevan avainasemassa uusia järjestelmiä käyttöönotettavissa. Erityisesti perinteisten käyttäjän tunnistautumistapojen korvautuminen uusilla ja käyttäjätietojen laajempi hallinta

tunnistettiin työryhmätyöskentelyssä tulevaisuuden haasteeksi. Alueellisessa tietohallintosuunnitelmassa todettiin, että laitteiden keskimääräinen käyttöikä vaihteli erittäin nopeasta 3 vuoden kierrosta aina 7 vuoden kiertoon saakka. Työryhmätyöskentelyssä todettiin, että uusien järjestelmien käyttöönotolla on pakottava vaikutus laitteistokannan uusiutumiseen, vaikka resursseja ei uusimiseen olsikaan varattu tai vaihtoa suunniteltu. Organisaatioiden toimintayksiköiden itsensä hankkimat järjestelmät pahentavat tilannetta.

1.7.2 Aikataulutus

Työkokonaisuuden aikataululle selvimmät rajat asettaa Satakunnan Erityishuoltopiirin yhdistyminen 1.1.2009 alkaen ja Kansallisten järjestelmien käyttöönotto. Työkokonaisuudelle laadittiin jaksotus seuraavasti:

Esiselvitys	syksy 2007 - kevät 2008
Määrittely, PoC	04/2008
Käytännön toteutus	04 - 06/2008
Pohjaratkaisu valmiina	1.6.2008
Pilotoinnin alku	06/2008
Pilotoinnin loppu	08/2008
Korjaukset, jatkopilotti	09-10/2008
Valmis tuotantoon	11/2008
Ensimmäinen asiakas	12/2008 (osin SATSHP)
Toinen asiakas	01/2009 (SATAEHP)

Aikataulu koettiin haasteelliseksi mm. pilotointiajan alkamiseksi kesälomasesongin kynnyksellä. SATSHP:n rooli ensimmäisenä asiakkaana todettiin suunnitteluvaiheessa ongelmalliseksi organisaation suuren koon vuoksi. Tärkeimmäksi tavoitteeksi sovittiin Satakunnan Erityishuoltopiirin onnistunut sulauttaminen. Erityishuoltopiirin järjestelmien kartoitusta jatkettiin koko työkokonaisuuden ajan.

2 PALVELUVERKKO

Ensimmäisissä palveluverkon hahmotelmissa toteutuksesta rajattiin pois operatiiviset sovellukset ja Palveluverkko-konsepti rajattiin koskemaan vain perustietotekniikan palveluita. Kaikkien operatiivisten sovellusten vaatimusten huomioiminen perustietotekniikkahankkeessa koettiin mahdottomaksi. Palveluverkon rakenteesta päätettiin tehdä mahdollisimman monipuolinen ja samalla kuitenkin yksinkertainen huomioiden tulevat järjestelmähankkeet.

Ratkaisuvalintoja tehtäessä päätettiin hydöyntää SATSHP:n ja muiden toimijoiden kokemuksia eri järjestelmistä. Uusi ja tuntematon järjestelmä luokiteltiin riskiksi, kuitenkin siten, että järjestelmän mahdollisuuksia tulee tutkia objektiivisesti ilman ennakkokäsityksiä. Lähtökohtaisesti Palveluverkon ytimen muodostaa Satakunnan Sairaanhoitopiirin nykyisen Tietopalvelut-yksikön henkilöstö ja sen perustietotekniikasta siirrettävät laitteistot ja palvelut. Sairaanhoitopiirin järjestelmät ja laitteet on tuotantokäytössä toimiviksi todettu. Työryhmätyöskentelyssä todettiin kuitenkin, että hankituista laitteista ja ohjelmistoista ei saada kaikkea hyötyä ja asioita tehdään liikaa käsityönä ja ilman suunniteltuja prosesseja.

Palveluverkon suurimpana tavoitteen ja samalla alueen organisaatioiden suurimpana uhkana on järjestelmien käytettävyyden romahtaminen, ongelmien eteenpäinsiirtäminen ja tietohallinnon johtamisen puute. Haastatteluissa tietohallintohenkilöt osasivat nimetä suuren määrän ongelmia, mutta samalla jokaisen ongelman korjaamisen estäviä seikkoja. Haastatteluiden ja työryhmän jäsenten tietojen perusteella selvisi, että tulevaisuuden pakollisista järjestelmähankkeista ei selvitä ilman suurta järjestelmäuudistusta.

Palveluverkko-työkokonaisuuden suunnittelu on aloitettu jo loppukesällä 2007, jolloin kerättiin tietoja palveluverkkoon siirrettävistä palveluista ja järjestelmistä. Lisäksi ostettiin konsultointipalveluita perustietotekniikkapalveluihin erikoistuneilta yrityksiltä laajemman näkökulman saamiseksi. Työryhmätyöskentelyssä selvisi, että Palveluverkon laajuisia perustietotekniikan uudistamishankkeita on käynnissä Suo-

messa useita. Käytännön työ organisoitui OTO-menettelyksi. Kunkin osa-alueen asiantuntijat osallistuivat työryhmätyöskentelyyn ja käytännön asennustoimintaan mahdollisuuksiensa mukaan.

2.1 Palveluverkon tavoitetila

Työn alkuvaiheessa laadittiin palveluverkon tavoitetilan kuvaus. Tavoitetilaksi kuvattiin seuraavat asiakokonaisuudet:

- Palveluverkon järjestelmät on rakennettu geneeristen, palveluarkkitehtuuriin pohjautuvin järjestelmien ja ratkaisujen pohjalta, asiakaskohtaisesti räätälöityjä ratkaisuita pyritään välttämään.

- Perustietotekniikan palvelut tuotetaan vikasietoisilla, valvotuilla järjestelmillä ja laitteistoilla.

- Kaikilla Palveluverkon asiakkailla on yhtenevä perustietotekniikka, joka hankitaan kustannustehokkaasti Palveluverkon hankintakanavien kautta.

- Yhtenevän perustietotekniikan tuki- ja ylläpitopalvelut tuotetaan Palveluverkon organisaation kautta.

- Operatiivisten järjestelmien instansseja pystytetään vain tarvittava määrä, järjestelmät muokataan moniorganisaatiomallilla toimiviksi.

- Asiakasorganisaatioilla mahdollisuus hallita omia järjestelmiään.

- Palveluverkon asiakkaat sitoutetaan yhteiseen tietoturvapolitiikkaan.

- Palveluverkko toimii alueen luotettuna organisaationa esimerkiksi kansallisten järjestelmien käytössä.

- Palveluiden käytettävyyden tulee olla mitattavissa.

Tavoitetilaluettelo laadittiin palvelujen tuottamisen näkökulmasta ja tavoitteet asetettiin tekniikka- ja järjestelmäriippumattomasti. Tärkeimmäksi yksittäiseksi asiaksi tavoitetilassa todettiin yhtenevä perustietotekniikka. Perustietotekniikan hallinta on Alueellisen tietohallintosuunnitelman mukaan eniten IT-yksiköitä työllistävä osa-alue. Yhtenevän perustietotekniikan tuki- ja ylläpitopalveluiden tuottaminen on yksinkertaisempaa kuin hajanaisten laite- ja ohjelmistoversioiden hallitseminen. Perustietotekniikan kehittämisen tulokset ovat helposti siirrettävissä kaikkien asiakasorganisaatioiden käyttöön. Lisäksi todettiin, että ilman tavoitetilan mukaista järjestelmäkokonaisuutta ja perustietotekniikan uudistusta ei alueen terveydenhuollon toimijoilla ole edellytyksiä ottaa käyttöön lain edellyttämiä järjestelmiä, vastata palvelurakenneuudistuksen luomiin haasteisiin tai siirtyä sähköiseen arkistointiin.

Tietohallinnon kannnalta suurin muutos Palveluverkon käyttöönotossa on aikaisemmin käsityönä tehtyjen töiden, kuten ohjelmistopakettien jakelun, käyttäjätunnushakemusten paperilomakekäsittelyn ja työasemien perusasennuksen automatisointi. Yleisen käsityksen mukaan toimintojen automatisointi vähentää virheitä ja vapauttaa resursseja muihin tehtäviin. Tietoteknisen laitteiden kehittyessä erityisesti työasemalaitteistojen kohdalla on päästy tilanteeseen, jossa laitteistokomponenteilla tai laitteen valmistajalla ei ole suurta merkitystä. Alueellisen tietohallintosuunnitelman mukaan suurin osa alueen organisaatioista hyödynsi työasemalaitteistojen kohdalla joko laitevalmistajan tai jälleenmyyjän tukipalvelua asennus- ja ylläpitotilanteissa. Työryhmätyöskentelyssä todettiin prosessien automatisoinnin ja ulkopuolisten tukipalveluiden käytön siirtävän organisaatioiden omien tietohallintoresurssien työnkuvan muuttumista yhä enemmän järjestelmien hallinnan suuntaan, pois laitteiden käsittelystä. Organisaatioissa perinteinen mikrotukitehtävä on entistä enemmän sovellusten hallintaa, rutiiniluonteiset laitteisto- ja käyttöjärjestelmäonasiat ratkaistaan ulkopuolisen resurssin avulla ostopalveluna.

SATSHP:n Tietopalvelut-yksikössä on aikaisemmin tutkittu ITIL-konseptin hyötyjä ja käyttömahdollisuuksia toiminnan organisoinnissa. ITIL on lyhenne sanoista Information Technology Infrastructure Library ja se sisältää IT-projekteissa käytettäväksi tarkoitettuja prosessikuvauksia ja standardeja. Tietopalvelut-yksikön johtoryhmän linjauksen mukaan Palveluverkko-hankkeessa ei hyödynnetä ITIL-konseptia. ITIL-konseptin hyödyntäminen edellyttäisi koko yksikön toiminnan uudelleenorganisointia, johon ei toistaiseksi ole johtoryhmän päätöksen mukaan tarkoituksenmukaista ryhtyä.

Palveluverkon ytimen muodostaa Satakunnan Sairaanhoitopiirin käytöstä siirrettävät laitteistot ja järjestelmät, jolloin varsinaisia perustamiskustannuksia palveluverkolle tulee suhteellisen vähän. Suurimmat kuluerät tulevat päivitettyjen ohelmaversioiden käyttöoikeusmaksuista. Perustietotekniikan palvelut rakennetaan uudelleen toimimaan rinnakkain vanhan SATSHP:n järjestelmän kanssa. Satakunnan sairaanhoitopiirin ja Erityishuoltopiirin työasemia ja järjestelmiä siirretään Palveluverkkoon sitä mukaan kun operatiivisten järjestelmien käyttö sen sallii.

Alustavassa ryhmätyössä profiloitiin perustietotekniikan loppukäyttäjiä SATSHP:n asiakaspalvelun kokemusten ja asiakkaiden otoshaastattelun perusteella. Käyttäjäprofiilit pyrittiin pitämään mahdollisimman yksinkertaisina, jotta niistä olisi apua Palveluverkon määrittelytyössä. Käyttäjäprofiileiksi tunnistettiin seuraavat:

- "Tehokäyttäjät" - käyttäjät, joiden työtehtävät ovat moninaiset, käytettäviä järjestelmiä ja oheislaitteita on paljon, esimerkkinä johdon ja yleishallinnon sihteerit, Tietopalvelut-yksikön työntekijät, luottamusmies- ja työsuojeluorganisaatiossa työskentelevät, tekniikan suunnitteluosaston käyttäjät, sosiaalityöntekijät, media-assistentti.

- "Normaalikäyttäjät" - käyttäjät, joiden työtehtäviin kuuluu olennaisena osana tietojärjestelmien käyttö, käytettävät välineet eivät muutu: hoitajat, lääkärit, sihteerit, sairaala-apteekin henkilökunta, henkilöstö- ja laskentapalveluiden henkilöstö, osastonhoitajat, varastotyöntekijät, ravitsemustyöntekijät.

- "Satunnaiset käyttäjät" - käyttäjät, joiden työtehtävien hoitaminen ei edellytä jatkuvaa tietojärjestelmien käyttöä: laitoshuoltajat, kuljetusyksikön henkilökunta

- "Liikkuvat käyttäjät" - käyttäjät joiden työpiste vaihtelee, esimerkkinä päivystävät lääkärit, osa hallinon esimiehistä, Tietopalvelut-yksikön henkilökunta.

- "Ongelmakäyttäjät" - käyttäjät, jotka työskentelevät keikkaluonteisesti ja joiden työaika on yleensä Tietopalvelut-yksikön normaalin palveluajan ulkopuolella (ilta, viikonloppu): keikkalääkärit, vartijat.

Käyttäjäprofiilien laatimisesta huolimatta työryhmätyöskentelyssä todettiin, että kaikki loppukäyttäjät ovat tärkeitä ja heidän ongelmiinsa pitää suhtautua riittävällä vakavuudella. Perustietotekniikan uudistamisesta toivotaan apua kaikenlaisten käyttäjäryhmien päivittäisten ongelmien käsittelemiseen.

2.2 Palveluverkon toteutukseen vaikuttavat kehittämishankkeet

Tavoitetilan laatimisen jälkeen verrattiin asiakokonaisuuksia tiedossa olleisiin kehittämishankkeisiin ja tuleviin järjestelmiin. Perustietotekniikan kannalta huomionarvoisiksi todettiin seuraavat hankkeet:

- Kansallisten tietojärjestelmien ensimmäisten osien käyttöönotto 1.4.211 alkaen

- Sähköisen arkistoinnin mahdollistavan lain edellyttämät tietojärjestelmien käytettävyysvaatimukset

- Vaatimus käyttäjien vahvasta tunnistamisesta kansallisia järjestelmiä käytettäessä, Terveydenhuollon oikeusturvakeskuksen varmennepalve-

lu ja käyttöönotettavat Terveydenhuollon ammattihenkilöiden toimikortit

- Satakunnan Sairaanhoitopiirin potilastietojärjestelmän ydinosien uudistamishankkeen käynnistys

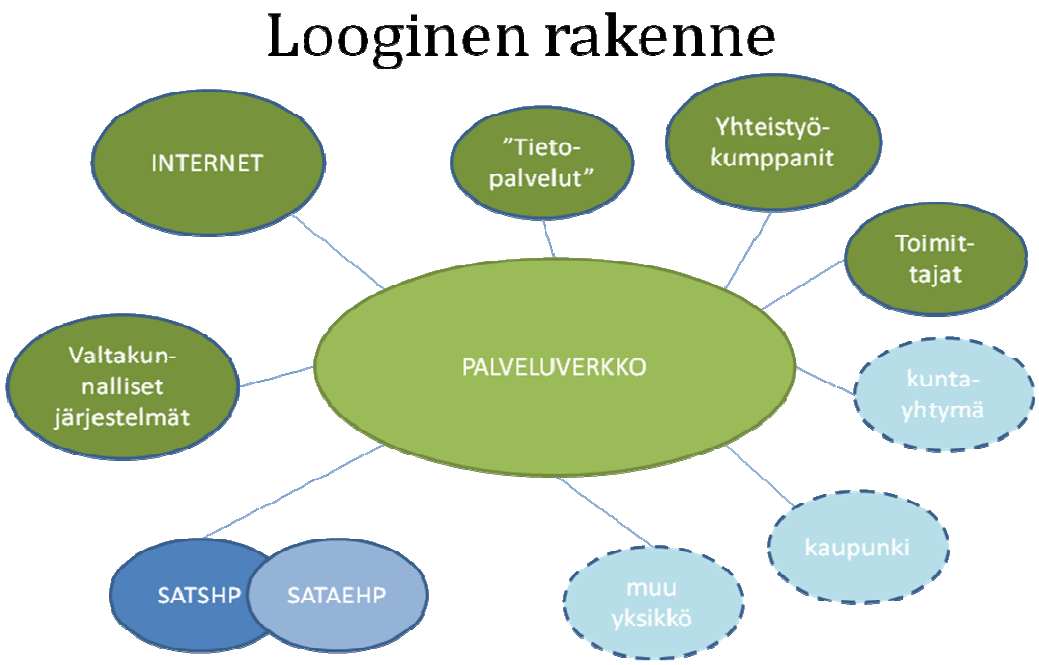
- Satakunnan Erityishuoltopiirin yhdistyminen Satakunnan Sairaanhoitopiiriin 1.1.2009 alkaen

- Satakunnan Sairaanhoitopiirin palvelurakenneuudistus

Työryhmätyöskentelyssä todettiin edellämainittujen hankkeiden aiheuttavan suuria muutospaineita perustietotekniikan lisäksi monille muille järjestelmille, kuten laskutus- ja tilastointisovelluksille, joiden rajapinnat on määriteltävä uudelleen. Monessa yhteydessä käsitelty käyttäjän vahva tunnistaminen luokilteltiin tavoitteeksi, jonka toteutumisesta ei voida luopua. Käytettävissä olevien materiaalien perusteella oli selvää, että kaikessa terveydenhuollon tietojenkäsittelyssä siirrytään vähitellen käyttäjän vahvaan tunnistamiseen.

2.3 Perusrakenne

Palveluverkon perusrakenne ja looginen kuva (Kuvio 1) muodostui varsin nopeasti. Suurin muutos olemassaolevaan tapaan toimia on Sairaanhoitopiirin siirtyminen asiakkaan rooliin ja Tietopalvelut-yksikön siirtyminen pois Sairaanhoitopiiristä Palveluverkkoa hallinnoivaan rooliin. Palveluverkon rakennetta esiteltiin laajemmalle yleisölle ensimmäisen kerran 29.5.2008, jolloin kuulijakunta muodostui Satakunnan kuntien ja kuntayhtymien tietohallintojohdosta ja asiantuntijoista.



Kuvio 1. Palveluverkon looginen rakenne ja toimijoiden väliset suhteet

Asiakkaat ja Palveluverkon yhdistävät tietoliikenneyhteydet mitoitetaan asiakasorganisaation käyttötarpeen, järjestelmien ja organisaation koon mukaan. Järjestelmien tietoliikenneyhteyksien kapasiteettivaatimukset selvitetään järjestelmätoimittajalta tapauskohtaisesti. Asiakasorganisaatiot voivat halutessaan luopua kaikista omista tietoliikenneyhteyksistään ja käyttää Palveluverkkoon rakennettuja yhteyksiä. Tietoliikenneyhteyksissä pyritään hyödyntämään reititettyjä ja vikasietoisia yhteyksien luontitapoja.

2.4 Palveluverkossa käytettävät järjestelmät

Palveluverkon perustietotekniikan palvelualustana käytettävät järjestelmät valittiin workshop-tilaisuuksien keskustelujen, konsulttien esitysten, tavoitetilaluettelon ja vertailujen pohjalta. Alun perin vertailu oli tarkoitus tehdä tekniikkariippumattomasti, eli kriteerinä olisi pidetty vain järjestelmän sopivuutta kyseiseen toimintoon. Järjestelmien vapaata valintaa rajoittivat mm. seuraavat asiat:

- Osa käytössä olevista tietojärjestelmistä on integroitu Microsoftin eri tuotteisiin.

- Käytännössä kaikki operatiiviset sovellukset on ja oheislaitteiden ajurit tehty käytettäväksi Microsoft Windows -käyttöjärjestelmällä, versioita muihin käyttöjärjestelmiin ei ole saatavilla.

- Käytössä olevat selainpohjaiset järjestelmät käyttävät Microsoft Internet Explorer -selaimen laajennuskomponentteja käyttöliittymän monipuolistamiseksi.

- Terveydenhuollon yksiköissä on käytössä paljon suoraan tietokoneeseen liitettäviä oheislaitteita, kuten digitaalisia sanelimia ja telemetria- ja muita mittauslaitteita, joiden käyttäminen terminaaliyhteyksien kautta ei onnistu.

Edellämainitut rajoitukset huomioiden loppukäyttäjien perustietotekniikkajärjestelmien tulee rakentua Microsoft Windows -käyttöjärjestelmälle ja yhteensopiville sovellustuotteille. Palveluverkon verkon peruspalveluita voidaan tuottaa muillakin järjestelmillä edellämainitut rajoitukset huomioiden.

Huomioitavaa on myös, että SATSHP:llä ja sen seurauksena Palveluverkolla ei ole käytössään Microsoftin Enterprise Agreement -sopimusta (EA) vaan Microsoft -järjestelmien lisenssointi toteutetaan Volume Licensing ja Select -hankintaohjelmien mukaisesti. Microsoft EA -sopimus mahdollistaa lisensoitujen Microsoft-tuotteiden laajan käyttöoikeuden ja ylläpidon sopimuskauden aikana. Volume Licensing ja Select -ohjelmat tarkoittavat käytännössä yksittäisten ohjelmistokäyttöoikeuksien hankkimista.

2.5 Palveluverkon palvelut

Palveluverkko tuottaa ja järjestää kaikki perustietotekniikan toiminnan edellyttämät palvelut. Suurin osa palveluista liittyy läheisesti toisiinsa, jolloin yksittäisiä palveluita ei ole kaikissa tapauksissa mahdollista jättää pois. Asiakasorganisaatioilla on mahdollisuus valita hallinnoinnin taso - ostetaanko kaikki hallinnointi palveluna vai säilytetäänkö omalla organisaatiolla mahdollisuus hallita rakenteita. Oletusarvoisesti hallinnointi on Palveluverkon tuottama palvelu.

2.5.1 Konesali- ja palvelinpalvelut

Palveluverkon palvelinlaitteet sijoitetaan Satakunnan keskussairaalan kahteen konesaliin. Konesalien talotekniikka- ja tietoliikenneyhteydet on mahdollisuuksien mukaan kahdennettu ja rakennettu vikasietoisiksi. Konesalipalvelu mahdollistaa myös palveluverkon asiakkaiden omien laitteiden sijoittamisen konesaliin.

Palvelimet on konsolidoitu fyysisen tilan säästämisen, energiansäästön ja virtualisoinnin mukanaantuomien teknisten mahdollisuuksien vuoksi. Palvelinlaitealustana käytetään VMWare ESX-virtualisointiympäristöä. VMWare-ympäristö mahdollistaa fyysisten laiteresurssien joustavan käytön eri palvelimien kesken. Laiterikon sattuessa virtuaalipalvelimia on mahdollista siirtää fyysisestä palvelinlaitteesta toiseen palvelimien rautakomponenttien ollessa yhteensopivia.

VMWare-virtualisointitekniikka on osoittautunut SATSHP:n käytössä toimivaksi, riittävän suorituskykyiseksi ja vikasietoiseksi. Järjestelmän käyttöjärjestelmätuki on laaja ja lähes kaikkien ohjelmistovalmistajien tuotteet on hyväksytetty käytettäväksi VMWare-virtuaaliympäristössä. Lähtökohtaisesti kaikki Palveluverkon palvelmiet virtualisoidaan. Poikkeuksena virtualisointisääntöön on yleisesti tunnustettu käytäntö järjestelmien vikasietoisuustason nostamiseksi siten, että kahdennetuista palvelimista toinen on oma fyysinen palvelimensa ja toinen on virtualisoitu palvelin. Näin menetellään verkon kriittisimpien palveluiden kohdalla.

Palvelinpalvelut-kokonaisuuteen sisältyy verkon peruspalveluita, kuten DHCP- ja DNS-palvelut sekä järjestelmien julkaisupalvelut kuten Citrix Metaframe. Verkon peruspalvelut tuotetaan vähintään kahdennetulla laitteistolla, jolloin laitteiston tai ohjelmiston vikaantuessa käyttökatkon mahdollisuus tai katkoon kuluva aika vähenee oleellisesti.

Lähtökohtaisesti palvelinpalvelut tuotetaan Palveluverkon määrittämillä ja käyttämillä palvelinlaitteilla, mutta poikkeustapauksissa palvelua tuotetaan asiakkaan Palveluverkon konesalipalvelussa olevilla laitteilla. Yhtenäisen käytännön ja määriteltyjen laitteiden käytöllä pyritään mahdollisimman lyhyisiin käyttökatkoihin ja korjausaikoihin. Käytännössä vakiintunut tapa on rakentaa jokaiselle operatiiviselle sovellukselle oma palvelimensa, jolloin yhden laitteen tai järjestelmän ongelmat eivät oletusarvoisesti aiheuta ongelmia muille järjestelmille.

2.5.2 Työasemalaitteistopalvelut

Palveluverkon loppukäyttäjälle näkyvin osa on työasema ja siihen liittyvät tukipalvelut. Työasemalaitteistopalvelut kattaa kaikki loppukäyttäjän tietojenkäsittelylaitteet: mikrotietokoneen, näytön, ohjauslaitteet, älykortinlukija, tulostimet. Työasemien käyttöjärjestelmän ja ohjelmistojen asentamisessa otettiin käyttöön asennusjärjestelmä, jolla asennuspaketteja voidaan hallita Active Directoryn Group Policy -objektein. Työasemassa käyttäjä tunnistetaan toimikortin avulla, perinteinen käyttäjätunnus-salasana -yhdistelmä on oletusarvoisesti poissa käytöstä.

Koska operatiivisten sovellusten määrä on laaja, niiden testaamiseen Palveluverkon työasemamallilla ei voida etukäteen tehdä. Työasemamallista tehdään kaksi eri käyttöjärjestelmäversiota, Windows XP- ja Vista -käyttöjärjestelmillä. Ensisijaisesti työasemissa käytetään Windows Vista -käyttöjärjestelmää, mutta operatiivisten sovellusten niin vaatiessa yksittäistapauksissa käytetään Windows XP -järjestelmää. Ohjelmistopakettien asennus automatisoidaan. Oletusarvoisesti kaikkia operatiivisia

sovelluksia ei asenneta kaikkiin työasemiin, vaan asennuksia ohjataan työasemien ryhmittelyllä

2.5.3 Työryhmäohjelmistopalvelut

Työryhmäohjelmistopalvelut tuotetaan Microsoft Exchange Server 2007 -järjestelmällä. Työryhmä vertaili eri työryhmäohjelmistotuotteita ja pyysi ulkopuolisen asiantuntijan kannanoton työryhmäohjelmistoasiaan. Exchange Server oli selvä vaihtoehto keskitetyn hallintansa ja laajan käyttäjäkunnan pohjalta. Työryhmäohjelmistona käytetään oletusarvoisesti Microsoft Exchange Server web-palvelua, aikaisemmalta nimeltään Outlook Web Access. Outlook-client -ohjelmisto asennetaan vain käyttäjäprofiililtaan "tehokäyttäjiksi" tunnistetuille käyttäjille. Testeissä Web-palvelun käytettävyyden todettiin olevan niin lähellä Outlook-client -ohjelmistoa, että käyttäjäprofiililtaan "normaalikäyttäjän" käyttökokemuksen ja järjestelmän käytettävyyden ei todettu olennaisesti heikkenevän.

Web-ohjelmisto todettiin ominaisuuksiinsa nähden myös selväksi kustannussäästöksi. Web-ohjelmiston käyttöön tarvitaan vain Microsoft Exchange Server CAL (Client Access Licence). Outlook-client -ohjelmiston todettiin tarvitsevan Exchange Server CAL -käyttöoikeuden lisäksi Outlook-client -käyttöoikeus. Microsoft Exchange Server integroituu Microsoft Active Directory -palveluun. Exchange Server -palvelun ja se käyttäjien hallinnassa on mahdollista käyttää Active Directory -ryhmäkäytäntöjä.

2.5.4 Internet-palvelut

Internet-käyttöä varten Palveluverkolla on käytössään kaksi internet-liittymää. Toinen liittymä on varattu normaaliin web-selailuun ja toinen palvelutuotantoon. Asiakasorganisaatioille on mahdollista varata internet-kapasiteettia haluttuun käyttötarkoitukseen (esim. videoneuvottelu). Internetin web-selailua rajoitetaan tietoturvapolitiikan mukaisesti.

Asiakkaiden käyttöön varataan tarvittavat internet-domain -nimet ja järjestetään nimipalvelut. Nimipalvelusta vastaava järjestelmä rakennetaan siten, että internet-domainia hallitseva primäärinimipalvelin on Palveluverkon hallinnassa ja nimipalvelun sekundääri- ja tertiäärinimipalvelut ostetaan palveluna internet-operaattorilta. Tällöin Palveluverkko voi itse ylläpitää nimipalvelimen tietoja, jotka replikoituvat automaattisesti operaattorin palveluihin.

2.5.5 Tietokantapalvelut

Oletusarvoisesti perustettavien tietokantojen hallintajärjestelmänä on Microsoft SQL Server 2005. Kaikki operatiivisten sovellusten tietokannat pyritään sijoittamaan tietokantapalvelimille luotaviin instansseihin. Uusia tietokantapalvelimia luodaan tarpeen vaatiessa. Tietokantapalvelimien resursseja ja kapasiteettia tarkastellaan valvontaohjelmiston avulla.

Kaikkia käytössä olevia järjestelmiä ei ole mahdollisuutta siirtää Microsoft SQL Server tietokannan hallintajärjestelmälle. Osa tietojärjestelmistä on toteutettu tietokantajärjestelmien omilla suunnittelutyökaluilla (mm. Oracle, Caché). Näitä poikkeustapauksia varten rakennetaan omat palvelimensa.

2.5.6 Varmistuspalvelut

Terveydenhuollon tietojen oikeellisuudesta ja saatavuudesta säädetään useassa lainkohdassa. Toistaiseksi sähköinen tietojen arkistointi ei ole hyväksytty arkistointimuoto, joten kaikki arkistoitava tieto on tulostettava paperille. Laki sähköisestä terveydenhuollon tietojen arkistoinnista on valmisteilla. Käytännön toteutuksena on Kansallinen Arkisto -tietojärjestelmäkokonaisuus.

Kaikki muuttuva tieto pyritään sijoittamaan Network Attached Storage (NAS) -laitepalveluun. NAS-järjestelmän tiedot kopioidaan kerran vuorokaudessa toiseen NAS-laitepalveluun, josta tiedot kopioidaan varmistusjärjestelmärobotin kautta perinteisille varmistusnauhoille. Tällöin tiedoista on olemassa alkuperäisen tiedon lisäksi kahdet eri kopiot, joita säilytetään eri palotilassa. Kuvattu varmistusmenettely on ollut SATSHP:ssä käytössä kolme vuotta. Ajanjakson aikana kaikki palautettava tieto on saatu ensimmäisestä kopiosta, eikä tietoja ole tarvinnut hakea varmistusnauhoilta. Tämä menettely nopeuttaa tietojen palautusta. Alun perin menettelytapaan päädyttiin tietojärjestelmien varmistusaikaikkunan muututtua riittämättömäksi. Tietojen kopiointi NAS-järjestelmästä toiseen on huomattavasti nopeampaa kuin suoraan NAS-järjestelmästä varmistusjärjestelmärobotin kautta varmistusnauhoille.

NAS-laitepalvelussa on sisäänrakennettu ohjelmisto, joka tallentaa halutuista levyresursseista määrävälein tilannekuvia (engl. snapshot) kahden viikon ajalta. Tilannekuvista levypalveluiden käyttäjät voivat itse palauttaa tiedostoja tiedostonhallintasovelluksen kautta.

Ne tiedot, joita ei voida sijoittaa NAS-laitepalveluun, varmistetaan palvelimen käyttöjärjestelmän kautta varmistusagenttiohjelmistolla. Tietokannat varmistetaan nk. dumpista, jolloin tietokanta pysäytetään ja sen sisältö transaktio- ja journal -lokitietoineen tallennetaan varmistusjärjestelmään. Mikäli tietokantaa käyttävä tietojärjestelmä on tunnistettu käytettävyystasoltaan kriittiseksi järjestelmän osaksi, sen tiedot varmistetaan nk. hot-backup -menettelyllä. Tällöin hyödynnetään varmistusjärjestelmän tietokannan hallintajärjestelmään sovitettua varmistusagenttia, jolloin tietokantatoimintoja tai järjestelmän käyttöä ei tarvitse keskeyttää.

2.5.7 Levypalvelut

Levypalvelut toteutetaan Network Attached Storage (NAS) -laitepalveluna. Levypalveluissa käyttöoikeuksien määrittely toteutetaan Windows-käyttäjäryhmiä ja Active Directory -käytäntöjä hyödyntäen. Levypalveluiden tilankäyttöä valvotaan ja sen

käyttäytymistä seurataan automatisoidulla tekniikalla jonka antamien raporttien pohjalta levypalveluiden resursseja muutetaan.

Levyresurssien jakamisessa hyödynnetään Microsoft Windows DFS -palvelua (Distributed File System). DFS-palvelun avulla levyresurssit on helposti siirrettävissä palvelimelta toiselle, resursseista voidaan tehdä vikasietoisia ja DFS-palvelua voidaan käyttää esimerkiksi asennusresurssin replikoinnissa useampaan eri asennuspisteeseen. Loppukäyttäjälle DFS-palvelun käyttöönotto näkyy ensisijaisesti lukumäärältään vähentyneinä levyresursseina.

2.5.8 Tietoliikennepalvelut

Palveluverkon tietoliikennepalvelut toteutetaan ensisijaisesti alueen teleoperaattoreilta ostettavilla palveluilla, joihin kuuluu myös yhteyden päätelaitepalvelu. Ensisijaisena yhdistämistekniikkana on reititetty yhteys operaattorin MPLS-verkon kautta. Lähtökohtaisesti kaikki muista tietoliikenne- ja verkkolaitteiden tuesta, käytöstä ja ylläpidosta vastaa Palveluverkko.

Tietoliikennepalvelut-kokonaisuus sisältää myös lähiverkko- ja runkoverkkolaitteiden ylläpidon. Lähiverkko- ja runkoverkkolaitteet sekä verkkoyhteydet määritellään valvontajärjestelmään, jonka kautta yhteyksien tilaa valvotaan automaattisesti.

Tietoliikennepalvelut tarjoaa myös asiakkaille etätyö- ja mobiilikäyttöön soveltuvat ratkaisut. Ratkaisuissa hyödynnetään standardeihin perustuvaa Mobile IP- ja IPSec-VPN -ratkaisua. Lähtökohtaisesti hitaiden yhteyksien kautta pyritään käyttämään terminaaliyhteyksiä tai Citrix-ympäristöä ja välttämään suoria yhteyksiä levyresursseihin ja järjestelmiin. Laite- ja järjestelmätoimittajien etähuoltoyhteydet rakennetaan toimittajien kanssa yhteistyönä lähtökohtaisesti VPN Lan-to-Lan -toteutuksin. Etähuoltoyhteyksien kohteet pyritään sijoittamaan liikenteen hallinnan ja pääsynvalvonnan mahdollistamiseksi omiin verkkoalueisiinsa.

2.5.9 Tietoturvaohjelmistopalvelut ja tietoturvapolitiikka

Palveluverkon asiakkaille rakennetaan keskitetty tietoturvaohjelmistopalvelu. Tietoturvaohjelmisto sisältää työasemille ja palvelinlaitteille yleisen käytännön mukaiset välttämättömät turvaohjelmistot: virustorjunta- ja palomuuriohjelmiston. Palveluverkon ja asiakasorganisaatioiden käytössä on myös verkkotason tietoturvajärjestelmiä verkkoliikenteen seurantaan, sähköpostien tarkistamiseen ja www-liikenteen suodattamiseen.

Lähtökohtana on, että kaikki haittaohjelmat pysäytetään verkkotasolla ennen kuin työasemien ja palvelimien tietoturvaohjelmistojen on tarve reagoida niihin. Tunnistetusti suurimmat ongelmat aiheutuvat salattujen internet-yhteyksien kautta (mm. salatut web-sähköpostipalvelut) saapuneista haittaohjelmista. Verkkotason tietoturvajärjestelmät eivät kykene tarkistamaan salatun yhteyden kautta saapuvia tiedostoja. Salattujen internet-yhteyksien, kuten SSL-menettelyllä suojattu HTTP-liikenne (HTTPS), salaus puretaan vasta yhteyden avanneessa työasemassa. Tällöin HTTPS-kanavan läp ladatun tiedoston tarkistaa ensimmäisen kerran vasta työaseman tai palvelimen tietoturvaohjelmisto.

Palveluverkon esimmäisessä vaiheessa ei oteta käyttöön Network Access Policy -palveluita (NAP), joilla on mahdollisuutta tehdä verkkoon kytkeytyvälle laitteelle nk. terveystarkastus. Terveystarkastuksessa on mahdollista käytettävästä tuotteesta riippuen tarkistaa mm. tietoturvaohjelmiston tai käyttöjärjestelmän tietoturvapäivitysten ajantasaisuus. Terveystarkastusta läpäisemätön laite voidaan virtuaalisesti eristää muista verkon laitteista ja tarjota laitteelle pääsy vain järjestelmiin, joista ohjelmistot on mahdollista päivittää ajantasaisiksi. Tietoturva- ja muiden päivitysten jakelemista varten Palveluverkkoon pystytetään Microsoft Server Update Services (WSUS) -palvelu. WSUS-palvelun kautta on mahdollista jaa keskitetysti päivityksiä verkon Windows-laitteille. WSUS-palvelu pakotetaan käyttöön verkon Active Directory -ryhmäkäytännöin.

Palveluverkon määrittelyitä laadittaessa lähtökohtana oli, että kaikki verkon asiakkaat sitoutuvat tietoturvapolitiikan perustasoon. Perustason lisäksi olisi mahdollista asettaa asiakaskohtaisia käytäntöjä, ei kuitenkaan perustasoa heikentävästi. Muutok-

set hyväksyy Palveluverkon tietoturvaryhmä, joka samalla huolehtii muutosten täytäntöönpanosta. Tietoturvapolitiikassa asetetaan mm. rajoituksia internetin palveluiden käytölle ja määritellään järjestelmiin tunnistautumisen vaatimukset.

3 HAKEMISTOJÄRJESTELMÄ JA TOIMIALUEEN PERUSPALVELUT

Aikaisempien kokemusten ja tiedossa olleiden hankkeiden vaatimusten osalta oli selvää, että Palveluverkon sydämen muodostaa hakemistojärjestelmä. Hakemisto on tietomalli, johon kuvataan käyttäjien ja resurssien tietoja helposti käsiteltävään hierarkiseen muotoon. Nykyisten hakemistoratkaisuiden kantaisä on raskas X.500 -hakemisto ja sen käyttöön kehitetty Directory Access Protocol (DAP). Nykyään hakemistolla tarkoitetaan oletusarvoisesti DAP:n kevyempää versiota, LDAP-hakemistoa.

Palveluverkon hakemistoratkaisuksi valittiin aikaisemmin esitettyjen rajoitusten ja toiminnallisuusvaatimusten pohjalta Microsoft Active Directory -palvelu. Active Directory sisältää Windows-toimialueen peruspalveluiden lisäksi LDAP-yhteensopivan hakemiston, jota oletusarvoisesti käytetään Windows-toimialueen tietojen tallennukseen. Microsoft Windows Server -käyttöjärjestelmän tasoksi valittiin versio 2003. Käytettävissä olisi ollut myös Microsoft Windows Server 2008, mutta sen ei työryhmätyöskentelyssä todettu tuovan niin suuria uudistuksia toimialue- ja Active Directory -palveluihin, että sen käyttöönottosta olisi ollut työkokonaisuuden ja aikataulun kannalta merkittävää hyötyä. Lisäksi todettiin, että pilotin edetessä ja peruspalveluiden vakiintuessa 2008-version palvelut rakennetaan rinnalle ja jossain vaihessa ratkaistaan, päivitetäänkö Palveluverkon toimialue ja metsä 2008-toiminnallisuustasolle.

3.1 Lightweight Directory Access Protocol (LDAP)

LDAP on protokollan ja hakemiston nimitys. Hakemiston rakenne on hierarkinen puu, jossa ylimpänä on juuritaso. Hakemiston ja protokollan tarkoituksena on tarjota yksinkertainen mahdollisuus hakemistoon kirjattujen henkilöiden, laitteiden tai muiden resurssien paikantamiseen. LDAP-hakemiston käsittelyyn on monenlaisia työkaluja, yksinkertaisimmillaan LDAP-hakemistoa pääsee selaamaan web-selaimella.

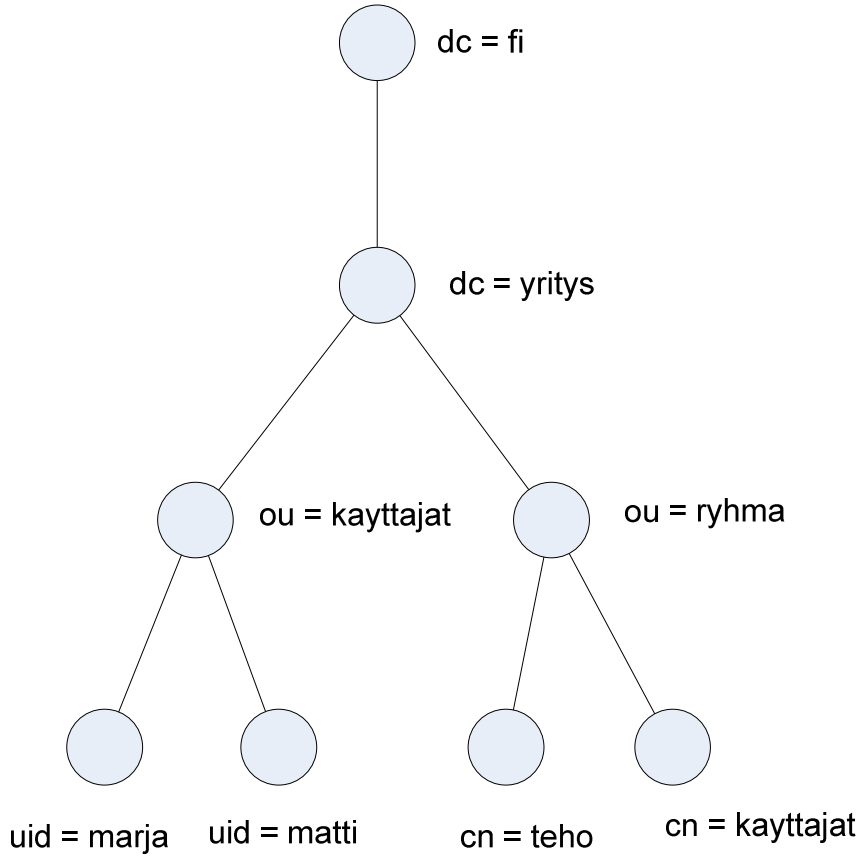
Hakemiston rakenne on tarkkaan määritelty. Taulukossa 1 on esitelty yleisimmin käytetyt LDAP-hakemiston attribuutit.

DN	Distinguish Name
UID	User id
CN	Common Name
SN	Surname
L	Location
OU	Organizational Unit
O	Organization
DC	Domain Component
ST	State
C	Country

Taulukko 1. Yleisimmät LDAP-attribuutit

LDAP-attribuuttien Yhdysvaltalainen historia vaikeuttaa attribuuttien suomalaista käyttöä. Hakemistoon on määritelty paljon attribuuteja, joita ei Suomessa voida hyödyntää tai niihin talletetaan kuvauksen vastaista tietoa.

LDAP-hakemistossa DN erottaa hakemiston organisaatiot toisistaan. Hakemisto voi sisältää siis monen eri organisaation tietoja. Analogiaa haettaessa Distinguish Name -attribuuttia voi verrata internetin domain-käsitteeseen. Seuraavassa kuviossa on kuvattu esimerkinomainen LDAP-hakemisto:



Kuvio 2: Esimerkki LDAP-hakemistosta.

DN muodostuu DC-komponenteista ylhäältä alaspäin edettäessä. Viitattaessa esimerkin "kayttajat" -organisaatioyksikköön, DN kirjoitetaan muotoon

ou=kayttajat,dc=yritys,dc=fi

Viittaus LDAP-hakemistossa olevaan objektiin "matti" voidaan kuvata myös URL-viittauksena:

ldap://ldaphaku.yritys.fi/ou=kayttajat,uid=matti,dc=yritys,dc=fi

Käytännössä hakemiston sisällä objektien lajittelu toteutetaan luomalla hierarkisia OU-säiliöitä hallinan ja tietoturvan kannalta tarvittava määrä. OU-säiliöiden lisääminen monimutkaistaa edellä esitettyjä LDAP-viittauksia. Huomioitavaa on myös joidenkin sovellusten asettamat rajoitukset LDAP-kyselyille. Tyypillistä on, että käytettäessä LDAP-hakemistoa käyttäjien tunnistamiseen sovellukseen on mahdollista asettaa vain yksi DN. Tällöin usean organisaation hakemistossa joudutaan DN aset-

tamaan puussa varsin ylös, jolloin laajoissa suurilla reaaliaikavaatimuksilla määritellyillä sovelluksilla kyselyjen suoritusajan venyminen voi aiheuttaa ongelmia.

3.2 Microsoft Active Directory (AD)

Microsoft Windows Server 2000:n yhteydessä julkaistu Microsoft Active Directory eroaa muista LDAP-hakemistoratkaisuista siten, että se ei ole pelkkä hakemisto, vaan kokoelma palveluita, jotka hyödyntävät palvelimen sisäistä hakemistoa. Hakemisto toteuttaa LDAP-standardin osia riittävällä tasolla ollakseen "LDAP-yhteensopiva" hakemistojärjestelmä. Kaikki nykyiset Microsoft Windows Server -verkkopalvelut kykenevät hyödyntämään Active Directory -palvelua tietojen keskitettynä tallennuspaikkana.

Active Directory muodostaa Windows-toimialueen ytimen, johon toimialueen käyttäjien ja laitteiden tiedot kirjataan. Active Directory -palveluun integroituvat ohjelmistot muokkaavat hakemiston rakennetta, schemaa, lisäten hakemistoon järjestelmän käytön kannalta tärkeitä attribuutteja ja rakenteita. Muista LDAP-tuotteista poiketen Active Directory käyttää hakemistonsa viittauksissa kirjoitusasua, jossa erottimena toimiva pilkku (",") on korvattu kautta-merkillä ("/").

Microsoft Windows Server 2008:ssa on mahdollisuus ottaa käyttöön Microsoft Active Directory Lightweight Directory Services -palvelu (LDS). Palvelu tarjoaa LDAP-yhteensopivan hakemiston ilman Active Directory -palveluita. LDS-palvelu soveltuu verkon reunalla tehtäviin hakemistopohjaisiin tunnistautumisratkaisuihin, joissa ei ole suoraa tarvetta muille Active Directory -toiminnallisuuksille.

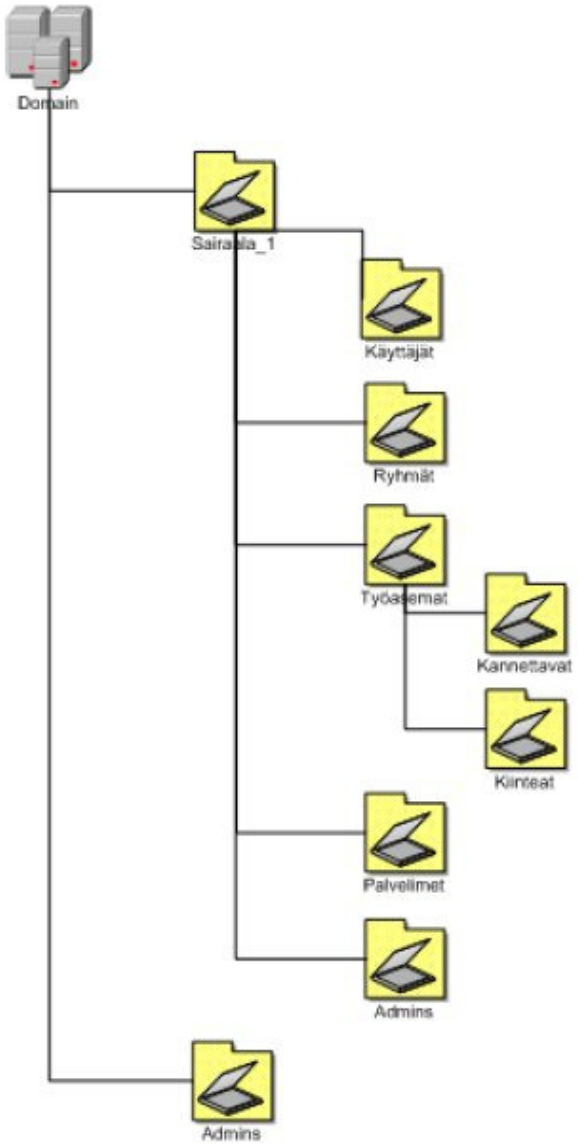
3.3 Palveluverkon Active Directory -hakemiston rakenne

Palveluverkon Active Directory muodostaa yhden metsän (forest) ja yhden toimialueen (domain). Toisiin toimialueisiin luodaan luottosuhteita vain välttämättömissä

tilanteissa. Tietoturvan kannalta luottosuhteiden rakentamista on harkittava tarkoin etenkin tilanteessa, jossa luottosuhteessa olevat toimialueet ja metsät ovat Active Directory -palvelun oletusasetuksialla. Tällöin toimialueen toiminnallisuustasosta riippuen metsien ja toimialueiden väliset transitiivisuusasetukset voivat aiheuttaa odottamattomia ongelmia.
(Microsoft, 2008)

Transitiivisuudella tarkoitetaan hierarkisessa metsärakenteessa puun haarojen luottamuksen periytymistä. Oletusarvoisesti Windows Server 2003 -toiminnallisuustason verkossa metsä ja toimialue ovat kokonaan transitiivisia, jolloin kahden metsän välille luotu kaksisuuntainen transitiivinen luottosuhde aiheuttaa ei vain metsän juuritason luottosuhteen vaan myös metsän alimpien haarojen keskinäisen luottamussuhteen. Luottosuhteen suunta ja erityisesti suhteen transitiivisuus tulee siis valita tarkoin. Metsän sisällä luottosuhteet ja transitiivisuusasetusten periytyminen voidaan katkaista hallinnan monimutkaistumisen kustannuksella.
(Microsoft, 2008)

Jotta palveluverkon hajautettu hallinta olisi mahdollinen, eikä eri asiakkailla ole mahdollisuutta nähdä tai käsitellä toistensa tietoja, toimialueen eri asiakasorganisaatiot erotellaan organisaatioyksikkötasolla. Jokaista asiakasorganisaatiota varten perustetaan juuritason alle oma organisaatioyksikkö, jonka alle sijoitetaan kuvio 3:n mukaiset organisaatioyksikköhaarat objektien säiliöiksi.



Kuvio 3. Palveluverkon Active Directory -hakemiston puurakenne

Jokaiselle hakemistoon perustettavalle asiakkaalle luodaan oma OU-rakenne, jonka hallinta voidaan tarvittaessa delegoida yksikön pääkäyttäjille. Hakemistoon luotavat Active Directory -objektit sijoitetaan OU-rakenteisiin seuraavalla jaottelulla: pääkäyttäjät, käyttäjät, käyttäjäryhmät, resurssit, kirjoittimet, työasemat ja asiakaskohtaiset palvelimet sekä sähköpostipalveluiden tarvitsemat objektit. Työasemiin kohdistettavien erilaisten hallinnointitarpeiden sekä esimerkiksi ohjelmistojakeluiden vuoksi työasemat sijoitetaan omien OU-rakenteiden alle siten, että myös työaseman malli erotetaan: pöytäkoneet, kannettavat.

Toimialuetasoiset objektit, kuten toimialueen pääkäyttäjät ja toimialueen ohjaustietokonetilit luodaan päätason säiliöihin. Acitve Directoryn hallintaoikeudet delegoidaan organisaatioyksiköille. Tavoitteena on mahdollisimman pieni Domain Admin -tason käyttäjien lukumäärä. Asiakasorganisaation pääkäyttäjillä on mahdollisuus hallita rajoituksin omaa organisaatioyksikköhaaraansa.

Active Directoryn rakennetta suunniteltaessa huomioitiin myös samannimisten objektien olemassaolon mahdollisuus. Hakemiston objekteille luotiin nimeämiskäytäntö, jolla objektit erotellaan toisistaan. Nimeämiskäytäntö on kuvattu taulukossa 2.

Objekti	Objektin nimeämiskäytäntö	Esimerkki ja kuvaus
Ryhmät	<lyhenne>g/l/u/d_<ryhmän_kuvaus> g = global, l = local, u = universal, d = distribution	SSPg_konekirjoittajat = global-ryhmä, Satakunnan Sairaanhoitopiiri, Konekirjoittajat-ryhmä
Käyttäjät	sähköpostiosoite <lyhenne><3etunimestä><2sukunimestä>	juha.salmi@satshp.fi SSPjuhsal = Satakunnan Sairaanhoitopiiri, Juha Salmi
Toimialueen pääkäyttäjät	adm.sähköpostiosoite adm<3etunimestä><2sukunimestä>	adm.juha.salmi@satshp.fi admjuhsal = pääkäyttäjä, Juha Salmi
Asiakas-organisaation pääkäyttäjät	sähköpostiosoite adm<lyhenne><3etunimestä><2sukunimestä>	adm.juha.salmi@satshp.fi admSSPjuhsal = Pääkäyttäjä, Satakunnan Sairaanhoitopiiri, Juha Salmi
Tietokoneet	<lyhenne>l/d/s<juokseva_numero> l = kannettava tietokone, d = työasema, s = palvelin	SSPL55432 = Satakunnan Sairaanhoitopiiri, kannettava tietokone, numero 55432
Tulostimet	<lyhenne>p<kuvaus>	SSPPTaltsto = Satakunnan Sairaanhoitopiiri, tulostin, Taloustoimisto
Group Policyt	<lyhenne>_gpo_c/u_<kuvaus> c = computer, u = user	SSP_gpo_c_JavaFix = Satakunnan Sairaanhoitopiiri, Computer Group Policy, JavaFix

Taulukko 2. Palveluverkon Active Directory -hakemisto-objektien nimeämiskäytäntö

3.4 Active Directoryn pääkäyttäjämäärittelyt

Toimialueen pääkäyttäjät erotetaan asiakasorganisaation pääkäyttäjistä. Toimialueen pääkäyttäjät luodaan juuritasolla olevaan Admins -organisaatioyksikköön. Aiakasorganisaatioiden pääkäyttäjät luodaan asiakasorganisaation organisaatioyksikköön ja nimetään nimeämiskäytännön mukaisesti. Organisaatioille luodaan taulukko 3:n mukaiset käyttäjäryhmät.

Pääkäyttäjäryhmä	Rooli
<Lyhenne>_SRV_Admins	Palvelinten pääkäyttäjät
<Lyhenne>_WS_Admins	Työasemien pääkäyttäjät
<Lyhenne>_OU_Admins	Organisaatioyksikön pääkäyttäjät
<Lyhenne>_WS_PowerUsers	Työasemien tehokäyttäjät
<Lyhenne>_Pwd_Admins	Salasanojen hallintaryhmä
<Lyhenne>_Comp_Admins	Työasematilien ylläpitoryhmä

Taulukko 3. Asiakasorganisaatioiden pääkäyttäjäryhmät

3.5 Toimialueen toiminnallisuudet

Microsoft Winodws Server -verkon peruspalvelut rakentuvat jälkeen roolipohjaisesti. Rooleja nimitetään FSMO-rooleiksi (Flexible Single Master Operations role). Windows-toimialue tarvitsee tietyt roolit perustoiminnallisuuden saavuttamiseksi. Kaikkia saatavilla olevia rooleja ei ole tarkoituksenmukaista ottaa käyttöön. Roolien lisäys ja siirto palvelimilta toiselle on mahdollista tehdä jälkeenpäin tarpeen mukaan. Windows-verkossa toimialuetta hallitsevia ja verkon asiakkaita palvelevia koneita nimitetään Domain Controller (DC) -palvelimiksi. Microsoft Windows Server 2000 -toimialuetoiminnallisuuden myötä aikaisempien Windows-toimialueiden suurin riskitekijä, nk. Primary Domain Controller -palvelimen (PDC) vikaantuminen ja muutoskyvyttömien Backup Domain Controller-palvelmien (BDC) varassa toimiminen, on on poistunut. Kaikkien DC-palvelimien on mahdollista ottaa vastaan muutoksia verkon asiakkailta ja niillä on kyky replikoida tiedot muiden toimialueen ohajuskoneiden kanssa. Microsoft Windows Server 2008:n myötä on mahdollista luoda kirjoitussuojattu Read-Only Domain Controller (RODC) -palvelin, jota voidaan käyttää

erikoistarkoituksiin, kuten käyttäjien yksisuuntaiseen tunnistamiseen verkon demilitarisoidulla vyöhykkeellä.
(Microsoft, 2008)

Palveluverkon peruspalvelut tuotetaan suunnitellusti kolmella palvelimella. Tärkeimmät verkon palvelut, Global Catalog ja DNS-palvelut asennetaan kaikille palvelimille. Muut FSMO-roolit asennetaan Microsoftin suositusten mukaisesti hieman hajauttaen taulukon 4 mukaisesti.

FSMO rooli	**DC01**	**DC02**	**DC03**
Schema Master		X	
Domain Naming Master		X	
Infrastructure Master	X		
PDC Emulator	X		
RID Master	X		
Global Catalog	X	X	X
DNS	X	X	X

Taulukko 4. FMSO-roolien jaottelu DC-palvelimien kesken

Schema Master (SM) vastaa Active Directoryn rakenteen, scheman, ylläpidosta. Schemaa on mahdollista muokata vain Schema Master -FSMO-roolin omaavalta palvelimelta. SM-palveluita voi Windows-metsässä olla vaín yksi. Domain Naming Master (DNM) huolehtii metsänlaajuisesta nimiavaruuden hallinnasta, toimialueiden liittämisestä ja poistamisesta. DNM välittää tiedon luottosuhteen yli luottosuhteen toiselle DNM-palvelulle. DNM-palveluita voi Windows-metsässä olla vain yksi.
(Microsoft, 2008)

Kaikilla Active Directory -objekteilla on oma yksilöllinen tunnisteensa (ID). Jokaiselle objektityypille on omanlaisensa tunniste. Päivittäisessä hallintatyössä käytetyimmät tyypit ovat SID (Security ID) ja GUID (Globally Unique ID). Molempien tunnisteiden luonnista ja hallinnasta vastaa Infrastructure Master -roolin palvelin. Uusia Active Directory -objekteja (esimerkiksi käyttäjätilejä) voidaan luoda miltä tahansa toimialueen ohjauskoneelta, jolloin jokaiselle ohjauskoneelle pitää määritellä oma ID-osoiteavaruus (pool). Osoiteavaruuden jaosta vastaa RID Master (Relative

ID Master). RID Master -rooli voi olla vain yhdellä toimialueen palvelimella. (Microsoft, 2008)

Moneen ohajuskoneen ympäristössä erityisen tärkeää on huolehtia siitä, että tietojen replikoituessa eri palvelimien ja tietosäiliöiden kesken, laitteiden kellonaika on synkronoitu. PDC Emulator huolehtii verkon yleisestä ajasta (Common Time). Yleisajan saatavuus on edellytys mm. Kerberos-autentikoinnille. PDC Emulator toimii myös vanhojen Microsoft Windows Server NT -toimialueen Primary Domain Controller -palveluna, jolloin mahdollisesti verkossa käytössä olevat vanhat Backup Domain Controller -palvelimien on mahdollista saada ajantasaiset tiedot.
(Microsoft, 2008)

Tärkein osa Active Directory -palvelun ja Windows-verkon asiakkaiden toiminnan kannalta on pääsy Global Catalog -palveluun. Global Catalog -roolin palvelin kykenee tunnistamaan mm. Windows-toimialueen laitteet ja käyttäjät. Global Catalog -palvelu on suuressa verkossa paljon käytetty, jolloin muiden roolien siirtäminen pois Global Catalog -palvelimilta on Microsoftin mukaan suositeltavaa.
(Microsoft, 2008)

Microsoft Windows Server 2000 -verkkopalveluiden myötä verkon toiminnallisuus on täysin riippuvainen DNS-palvelun (Domain Name Service) toiminnasta. Aikaisemmin käytetty NetBIOS-nimipalvelu on ongelmallinen reititettyjä tietoliikenneyhteyksiä käytettäessä. Windows Server 2000-toiminallisuustason myötä Windows-toimialue tarvitsee DNS-palvelun, joko Windows Server -palveluna tai muuna DNS-palveluna, esim. Linux-alustalla BIND-palvelimelta. Windows Server 2000 -toiminnallisuustason myötä oli myös mahdollisuus ottaa käyttöön Dynaaminen DNS -toiminnallisuus Windows-palveluilla. Dynaaminen DNS -palvelu tarkoittaa käytäntöä, jossa verkon asiakkaalle DHCP (Dynamic Host Configuration Protocol) -palvelun kautta annettujen IP-osoitetietojen ja DNS-palvelun välille voidaan rakentaa yhteys. Tällölin DHCP-palvelua käyttävien asiakkaiden laitteiden nimet on saatavilla automaattisesti DNS-palvelusta. Tämä on erityisen hyödyllistä järjestelmien tuki- ja ylläpitotehtävissä työskenteleville, jolloin koneen selväkielistä nimeä voidaan käyttää yhteyden muodostamisessa. DNS-palvelu asennetaan Palveluverkossa kaikille DC-palvelimille. IP-osoitetietojen jakelusta Palveluverkossa huolehtii oma palveli-

mensa. DHCP-palvelussa hyödynnetään reititettyjen tietoliikenneyhteyksien osalta DHCP Relay -toiminnetta, jolla levitysviestien kautta toimiva DHCP-järjestelmä (Microsoft, 2008)

Työasemien asennusjärjestelmää ja asennuspakettien hallintaa varten rakennetaan oma palvelin, jolloin oletusarvoisesti raskas asennusliikenne ei kuormita muita verkon hallintapalvelimia. Asennusjärjestelmänä käytetään Microsoft Windows Deployment Server -tuotetta (WDS) ja sen päälle rakennettuja Active Directory -ryhmäkäytäntöjä sekä skriptaustyökaluin tuotettuja apuohjelmia. Lähtökohtaisesti työasemien perustoiminnallisuus on kaikilla Palveluverkon asiakkailla sama, asiakas- ja laitekohtaisia muokkauksia on mahdollista tehdä.
(Microsoft, 2008)

Palveluverkon käytännön hallinta tukeutuu vahvasti Active Directory -ryhmäkäytäntöihin, jotka kohdistetaan AD-rakenteen mukaisesti kohdeorganisaatioon. Ryhmäkäytännöt ovat käytännössä viittauksia Windows-järjestelmän rekisterin avaimiin. Eri ohjelmistotuotteille on olemassa mallipohjia (Template), joiden viittauksista ryhmäkäytännöt luodaan. Mallipohjia on mahdollista luoda käsin lisää, mutta yleisimmin käytettäviin ohjelmistoihin on olemassa kattavasti valmiita malleja.

Palveluverkossa on sovittu ryhmäkäytäntöjen käytöstä seuraavaa:

- Ryhmäkäytäntöjen käyttämättömät osat poistetaan käytöstä.

- Pyritään pitämään objektikohtaisten ryhmäkäytäntöjen määrä mahdollisimman pienenä hallinnan helpottamiseksi (maksimissaan 6 ryhmäkäytäntöä objektia kohden).

- Periytymisen katkaisumenettelyä tulee välttää.

- Ryhmäkäytäntörakenteessa on valmiina yleiset käytännöt, Default-DomainPolicy ja Default Domain Controllers Policy, joihin ei tehdä muutoksia. Palveluverkon perusasetuksia varten luodaan oma Baseline -ryhmäkäytäntö.

4 POHDINTA

Työ edellytti erittäin laajan perustietotekniikka-alueen kokoamista yhteen helposti hallittavaksi ja ymmärrettäväksi kokonaisuudeksi. SATSHP:n järjestelmäkokonaisuuden ongelmat ovat tyypillisiä kuntayhtymille ja julkisen sektorin toimijoille: järjestelmien määrä on pikkuhiljaa lisääntynyt ja niitä on hankittu ikään kuin kaupan hyllyltä sen tarkemmin miettimättä niiden vaikutusta kokonaisuuteen ja suunnitelematta jatkotoimenpiteitä. Yllättäen on jouduttu tilanteeseen, jossa vaivoin hallittavissa olevista järjestelmistä on tullut päivittäisessä toiminnassa korvaamattomia. Tilanne, jossa pelkkä operatiivisen sovelluksen kunnostaminen ei riitä, vaan koko tietotekninen infrastruktuuri on suunniteltava uudelleen, on edessä monella julkisen sektorin toimijalla.

Erityisen haasten työlle antoi sille osoitetut rajalliset resurssit. Henkilöresurssit olivat käytössä oman työn ohella -menettelyn kautta, jolloin selkeätä työkokonaisuutta ei ollut mahdollista muodostaa. Käytännössä työ jäi yhden-kahden hengen ydintiimin eteenpäinvietäväksi vaikka käytännön rutiininomaisia asennus- ja muita toimenpiteitä ostettiinkin tuntityönä ulkopuolisilta asiantuntijoilta. Henkilöresurssien sitoutumisen puute ja tietyntasoinen työssä mukanaolleiden asiantuntijoiden muutosvastarinta aiheutti niin edelleen ongelmia.

Kokonaisuus eteni aikataulussa. Työvaiheet valmistuivat järjestyksessä ja ulkopuolisen asiantuntijan käyttö rutiiniluonteisissa työtehtävissä auttoi aikataulutavoitteen saavuttamista. Työn ollessa valmis lopullisen pilotin aloittamiseksi jouduttiin tilanteeseen, että aluenperin perustietotekniikan uudistamiseen tähdännyt hanke oli muuttunut konsultin ja yhden-kahden asiantuntijan testilaboratorioksi. Samassa yhteydessä saatiin sairaanhoitopiirin kuntayhtymän taholta tieto, että hankkeen toteuttamiseen varatut määrärahat on vedetty yksikön budjetista pois. Asia, jolla ei alun perin tunnistettu olevan vaikutusta työn etenemiseen, lamaannutti hankkeen jatkon.

Pitkällisten keskustelujen ja pohdintojen tuloksena Palveluverkko-työkokonaisuus päätettiin marraskuussa 2008 jäädyttää saavutettuun tilaan ja vapauttaa sille varatut resurssit. Keskusteluissa todettiin jäädyttämispäätöksen aiheuttamat ongelmat:

SATSHP:llä ei ole mahdollisuutta ottaa käyttöön kansallisia järjestelmiä tai sulauttaa SATAEHP:n järjestelmiä suunnitellusti.

Kun jätetään huomiotta jäädyttämispäätös ja verrataan alkuperäisiä tavoitteita ja saavutettua tulosta, voidaan sanoa, että työkokonaisuudessa luotu pohjaratkaisu on kunnossa. Laajempi pilotointi käytännön tilanteissa operatiivisten sovellusten kanssa paljastanee ongelmat suhteessa asiakkailla käytössä oleviin prosesseihin ja uudistettuun perustietotekniikkakokonaisuuteen. Kaikki perustoiminnallisuudet, joita hankkeelle asetettiin, testattiin ja näiden osalta saatiin hyvää tietoa jatkoa ajatellen.

Hankkeen keskeytyminen aiheutti välittömästi sen, että Erityishuoltopiirin yhdistyessä vuodenvaihteessa 1.1.2009 jouduttiin tekemään hätäratkaisuja välttämättömien toimintojen toteuttamiseksi. Käytännössä jouduttiin tilanteeseen, jossa joudutaan laskemaan kahden dokumentoimattoman ja aikansa omaa elämäänsä eläneen järjestelmän yhdistämisen aiheuttavia ongelmia saavutettavien hyötyjen sijaan. Yksittäisiksi tärkeimmiksi tavoitteiksi nimetyt Erityishuoltopiirin yhdistäminen ja vahvan käyttäjän tunnistamisen käyttöönotot epäonnistuivat. Organisaatioilla ei ole edellytyksiä ottaa käyttöön esimerkiksi kansallisia järjestelmiä nykyisellä perustietotekniikkaratkaisulla.

Edelleen voidaan todeta, että vasta vuosien varrella Palveluverkkoon siirrettävät operatiiviset sovellukset ja niiden yhteistoiminta sekä kansallisten järjestelmien käyttöönotto antaa vasta todellisen kuvan hankkeen pohjaratkaisun onnistumisesta ja toiminnasta. Palveluverkko-hanke herätti kuitenkin keskustelua ja hankkeen keskeyttämisen jälkeen on ollut havaittavissa muutoksia toimintatavoissa.

LÄHTEET

Finlex. 2008 . Ajantasainen lakitieto [verkkodokumentti]. Erikoissairaanhoitolaki [Viitattu 1.6.2007]. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/1989/19891062

SATSHP. 2006. Alueellisen tietohallintosuunnitelma.

SATSHP. 2005. Tietopalvelut-yksikön johtoryhmän muistiot.

SATSHP. 2006. Tietopalvelut-yksikön johtoryhmän muistiot.

SATSHP. 2007. Tietopalvelut-yksikön johtoryhmän muistiot.

SATSHP. 2008. Yleistetoa [verkkodokumentti]. Sairaanhoitopiiri. [Viitattu 1.6.2007]. Saatavissa: http://www.satshp.fi

Wikipedia. 2008. LDAP [verkkodokumentti]. LDAP [Viitatu 1.6.2007]. Saatavissa: http://www.wikipedia.org

Microsoft. 2008. MCITP Windows Server 2008 Server Administrator