

Arto Marjamaa

KÄYTTÄJÄTUNNUSTEN HALLINTA

Case Sote-Helmi

KÄYTTÄJÄTUNNUSTEN HALLINTA
Case Sote-Helmi

Arto Marjamaa
Opinnäytetyö
Kesä 2015
YLI3SY
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Yrittäjyyden ja liiketoimintaosaamisen koulutusohjelma

Tekijä: Arto Marjamaa

Opinnäytetyön nimi: Käyttäjätunnusten hallinta – Case Sote-Helmi

Työn ohjaaja: Sinikka Viinikka

Kesä 2015

Sivumäärä 59 + 7 liitettä

Päättötyön tekijä on töissä it-suunnittelija Haapaveden kaupungilla. Hän vastaa sosiaali- ja terveystieteiden Helmen tietotekniikasta terveydenhuollon osalta. Organisaatiossa oli selvästi tarve kehittää käyttäjätunnusten hallintaa.

Työn tavoitteena oli tutkia mahdollisia ongelmia nykyisessä käyttäjätunnusten anomisprosessissa ja hallinnassa. Ongelmia tutkimalla oli tarkoituksena luoda kehitys- ja parannusehdotuksia uudesta toimintatavasta. Tavoitteena oli siis kehittää nykyistä prosessia.

Terveysalan ollessa kyseessä tietoperustaan vaikuttaa hyvin voimakkaasti säädetetyt lait ja asetukset. Nämä määrittelevät myös osan teknisistä ratkaisuista, kuten salasanan monimutkaisuudesta, pituudesta ja vaihtovälistä. Salasanoista ja salasanojen muodostamisesta on olemassa paljon hyviä käytäntöjä ja muistisääntöjä.

Kehittämistehtävään soveltui hyvin laadullisen tutkimuksen menetelmät. Tekijä on tehnyt organisaatiossa työskennellessään omia havaintoja ja haastatellut epävirallisesti työkavereita. Tätä tiedonkeruuta täydennettiin kyselytutkimuksilla esimiehille ja verkko- ja Efficatunnuksia tekeville ylläpidon henkilöille.

Kerätty aineisto tuki tehtyjä havaintoja. Lisäksi esimiehiltä tuli muutamia erittäin hyviä ja toteuttamiskelpoisia kehittämissuhteita. Paras toteutusmalli tekniselle ratkaisulle löytyi naapurikunnan vastaavista käytännöistä. Tämän teknisen ratkaisun käyttöönottoa ja hintaa lähdetään selvittämään.

Avainsanat: käyttäjätunnus, käyttäjätunnuksen hallinta, salasana, käyttäjän tunnistaminen

ABSTRACT

Oulu University of Applied Sciences

Master Degree Programme in Entrepreneurship and Business Competence

Author: Arto Marjamaa

Title of thesis: Managing user rights – Case Sote-Helmi

Supervisor: Sinikka Viinikka

Summer 2015

Number of pages 59 + 7 attachments

Author is working at town of Haapavesi. He is responsible for healthcare ict in Sote-Helmi. There were clear need for develop better ways to manage user rights in the organization.

Object for the thesis was find out current problems in the process to request username for user. Taking closer look for possible problems that lies in the process and would help to make suggestions to improve current process.

Healthcare is strongly regulated by laws and decrees. These defines some of the technical solutions such as complexity and length of password and how often you need to change your password. There are lot of best practices and thumb rules how to create a good password and how to remember your password.

Qualitative research methods suits well for this case. While the author has been working in the organization he has done observation and unofficially interview his colleges. More data was also collected with survey for supervisors and people in the charge of ict.

Collected data supported notes made by observation. Supervisors gave few very good suggestions how to develop future system. The best solution to improve current system found from neighbor town. Technical solution they are using will be monitored and costs calculated.

Keyword: username, managing usernames, password, authentication

Lyhenteet

AD	Active Directory eli aktiivihakemisto. Windows Serverin osa, jota käytetään muun muassa käyttäjätunnusten hallintaan.
eArkisto	Sähköinen potilastietojen arkistointi.
eResepti	Sähköinen lääkemääräys.
Hoitosuhde	Hoitosuhde tarkoittaa terveydenhuollon ammattihenkilön ja potilaan välistä luottamuksellista suhdetta.
MPLS	MultiProtocol Label Switching, vikasietoinen reitittävä tietoverkko
OU	Organizational unit, aktiivihakemistopuun "hakemisto", joka voi sisältää uusia organisatorisia yksiköitä, käyttäjätilejä tai tietokonetilejä.
SaaS	Software as a Service, palveluna toteutettu tietojärjestelmä
Spirometria	Spirometriassa mitataan ventilaatiota eli keuhkojen tuuletuskykyä
UPS	Uninterruptible Power Supply, järjestelmä tai laite, jonka tehtävä on taata tasainen virransyöttö lyhyissä sähkökatkoksissa ja syöttöjännitteen epätasaisuuksissa huolimatta.
Web-tallennus	CGI:n toiminta ohjelma, jota käytetään muun muassa henkilöstöhallintaan (työsuhteet, kesälomat, poissaolot).

Sisällysluettelo

1 JOHDANTO.....	7
1.1 Toimeksiantaja.....	7
1.2 Sote-Helmen tietojärjestelmät.....	8
1.3 Sote-Helmen käyttäjät.....	11
1.4 Tutkimusongelma.....	12
2 TOIMINTAAN VAIKUTTAVAT LAIT.....	13
2.1 Lainsäädäntö.....	13
2.2 Terveystieteiden tietojärjestelmien erityispiirteet.....	14
2.3 Sähköinen lääkemääräys (eResepti) ja sähköinen potilastiedon arkisto (eArkisto).....	17
3 SOTE-HELMEN KÄYTTÄJÄTUNNUSTEN HALLINTA.....	19
3.1 Helmen tekniset ratkaisut.....	19
3.2 Käyttäjätunnusten hallinnointi.....	20
3.3 Nykyinen tunnusten anomisprosessi.....	21
3.4 Käyttäjän todentaminen.....	24
3.5 Active Directory.....	26
3.6 Kertakirjautuminen.....	27
4 TUTKIMUS JA TULOKSET.....	29
4.1 Tutkimuksen teko.....	29
4.2 Kyselytutkimus esimiehille.....	30
4.2.1 Käyttäjätunnusten anomiseen liittyvät kysymykset.....	36
4.2.2 Käyttäjätunnusten hallintaan liittyvät kysymykset.....	39
4.3 IT-tiimin haastattelut.....	42
4.3.1 Kyselytutkimus ylläpidolle.....	43
4.4 Omat havainnot.....	45
5 KEHITYSSUUNNITELMA.....	48
5.1 Sähköinen järjestelmä.....	49
5.2 Web-tallennus.....	50
5.3 Aktiivihakemiston hallintaoikeuksien delegointi.....	53
6 YHTEENVETO JA POHDINTA.....	55
LÄHDELUETTELO.....	58
LIITTEET.....	60

1 JOHDANTO

Opinnäytetyön aiheeksi valikoitu käyttäjätunnusten hallinta useasta syystä. Organisaatiossa oli selkeä tarve kehittää käyttäjätunnusten hallintaa. Tätä tuki tekijän omat havainnot organisaation sisällä. Käyttäjätunnukset liittyvät oleellisesti tietoturvaan, joka on aina ajankohtainen asia. Tietoturvan rooli korostuu sosiaali- ja terveystoimen toiminnassa. Ajankohtaiseksi käyttäjätunnukset tekevät myös Sote-uudistus ja lait sähköisestä lääkemääräyksestä ja sähköisestä potilastiedon arkistosta, jotka toivat muutoksia organisaation käytäntöihin ja määrittävät käyttäjätunnusten ja salasanojen käytäntöjä. Aiheen valintaan vaikutti myös tekijän halu kehittää oman organisaationsa toimintaa ja tuottaa parannusehdotuksia havaittuun selkeään epäkohtaan.

Päättötyön tekijä on töissä Haapaveden kaupungilla ja vastaa sosiaali- ja terveystoimen Helmen tietotekniikan ylläpidosta pois lukien sosiaalitoimistot. Näin aihealue rajautui luonnostaan koskemaan vain Sote-Helmeä. Sote-Helmessäkin rajausta tarkentui koskemaan vain terveystoimea, koska sosiaalipuoli on it-päällikön vastuualueella ja sosiaalipuolen käyttämät ohjelmistot eriyvät osittain terveystoimen ohjelmistoista.

1.1 Toimeksiantaja

Tämän päättötyön toimeksiantajana on Haapaveden kaupunki, joka on perustettu 1866. Haapavedestä tuli kaupunki 1996. Asukkaita kaupungissa on 7238. (Haapaveden kaupunki 2014, viitattu 13.7.2014). Haapaveden kaupunki toimii isäntäkuntana sosiaali- ja terveystoimen Helmelle. Päättävä elin on kuntien yhteinen perusturvalautakunta, jossa on yksi edustaja jokaisesta kunnasta jokaista alkavaa 2000 asukasta kohti. Helmeen kuuluvat Haapavesi, Pyhäntä ja Siikalatvan (Kestilä, Piippola, Pulkki ja Rantsila) kunnat. Helmi vastaa kaikista laissa säädettyistä kansanterveys- ja sosiaalipalveluista ja niiden hallinnosta. Poikkeuksena Pyhännän kuntaa ostaa terveystoimen lisäksi vain rajatut sosiaalipalvelut. (Sosiaali- ja

terveyspiiri helmi 2014, viitattu 13.7.2014.)

Sote-Helmellä on alueellaan neljä terveyskeskusta (Haapavesi, Pulkkila, Pyhäntä ja Rantsila). Piippolan terveyskeskus suljettiin vuoden 2014 lopussa. Terveyskeskusten yhteydessä on lääkäripalveluiden lisäksi mielenterveysneuvola, a-klinikan palvelut, hammashuolto, neuvola ja fysioterapia. Haapaveden ja Pulkkilan terveyskeskuksissa on röntgen ja syyskuussa 2014 NordLabille ulkoistettu laboratorio. Kestilässä on hyvinvointipiste, joka tarjoaa hammaslääkäri, fysioterapia ja neuvolapalveluita. Terveyskeskusten yhteydessä on vuodeosastot Haapavedellä ja Pulkkilassa. Vanhainkoteja on kuusi; Paakkilanhovi Haapavedellä, Pihlajisto Kestilässä, Koivulehto Pulkkilassa, Vaarintalo Piippolassa, Nestori Pyhännällä ja Rantsilassa terveyskeskuksen yhteydessä oleva Kotipiha. Vanhainkotien lisäksi Helmen alueella on useita asumispalveluyksiköitä. Kehitysvammaisten asuntoloita on Haapavedellä, Kestilässä ja Rantsilassa. Toimintakeskuksia on Haapavedellä ja Rantsilassa. Rantsilassa on myös tukikeskus kuntoutujille. Lisäksi kouluterveydenhoitajilla on yksittäisiä työasemia Haapaveden, Pyhännän ja Siikalatvan kouluilla. Terveystalon magneettirekka käy Haapavedellä tekemässä magneettikuvauksia. Neuvoloissa on etälääkärin vastaanottoja.

Ympäristöpalvelu Helmi tuottaa elintarvike- ja terveysvalvontapalvelut, eläinlääkintähuollon palvelut ja ympäristönsuojelupalvelut. Eläinlääkärit löytyvät Haapavedeltä, Oulaisista ja Kestilästä. Elintarvike- ja terveysvalvonnan toimipisteet löytyvät Haapavedeltä, Pulkkilasta ja Oulaisista. Haapavedeltä löytyvät lisäksi ympäristönsuojelu ja vasta yhtiötetty ympäristölaboratorio Hakalab.

1.2 Sote-Helmen tietojärjestelmät

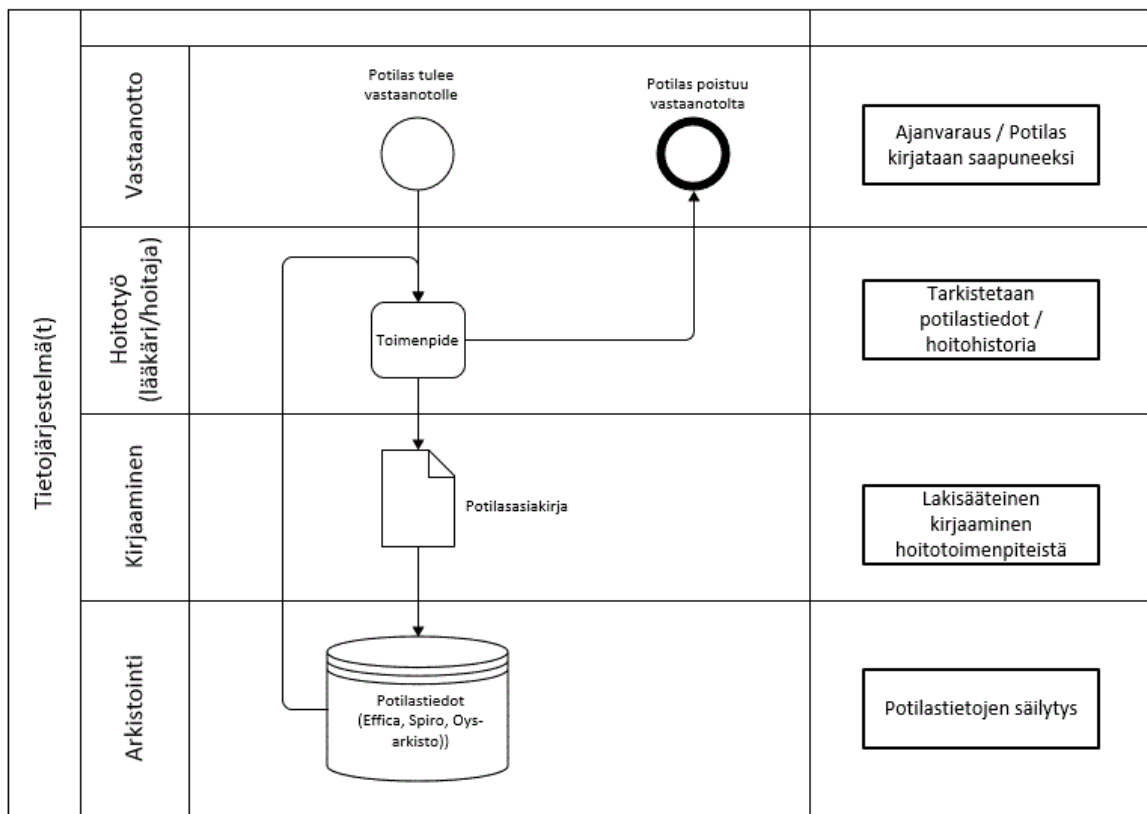
Sote-Helmessä on käytössä hyvin erilaisia tietojärjestelmiä. Osa järjestelmistä on valtakunnallisia, kuten eArkisto ja eResepti. Osa järjestelmistä on paikallisia, kuten spirometriassa käytettävä Spiro, potilastietojärjestelmä Effica, työvuorojen suunnitteluun käytetty Titania, matkalaskuohjelma ePopulus, lomien ja poissaolojen hallintaohjelma Web-

tallennus, hoitotarvikejakelu-ohjelmisto Effector ja sisäiseen tiedottamiseen tarkoitettu intranet. Jotkut tietojärjestelmät ovat ”yhteiskäytössä” toisen organisaation kanssa eli toimivat alueellisesti. Yhteiskäytössä ovat muun muassa potilastietojen siirtämiseen Sote-Helmen ja Oulaskankaan välillä tarkoitettu alue-Effica. Oulun yliopistolliseen sairaalaan (OYS) arkistoon viedään potilastiedot röntgenin NearIS-kuvantamisjärjestelmästä ja Romexis-hammashuollon kuvantamisjärjestelmästä sekä sydänfilmit suoraan EKG-laitteilta. Sote-Helmessä vieraileva Terveystalon magneettirekka välittää magneettikuvat myös suoraan OYS:n arkistoon Sote-Helmen tietoverkon kautta. OYS ylläpitää Eemeli-järjestelmää, josta alueen organisaatiot, Helmi mukaan lukien, tilaavat tarvikkeita. Osa järjestelmistä on ostettu SaaS-palveluna toimittajilta. Näitä ovat muun muassa lääkärin tietokannan tarjoava Terveysportti, puhelinpäivystysjärjestelmä TeleQ ja tietosuojan ja tietoturvan tenttiohjelmisto Navisec. Järjestelmiä käytetään internet-selaimella. Lääkäreille on työasemille asennettu digisanelu saneluja varten. Halutessaan lääkäreillä on sanelussa käytössä myös puheentunnistus. Sanelujen purkua varten sanelunpurkajien työasemille on asennettu polkimet, kuulokkeet ja sanelunpurkamiseen tarkoitettu ohjelmisto. Tilastotietoja ja seuranta varten Helmeen ollaan käyttöönottamassa Tieto Oyj:n toimittamaa uutta Effica-raportointia. Tätä järjestelmää käytetään internet-selaimella. Pääsyä rajataan verkkotunnuksilla ja käyttäjärhyhmillä (perus-, teho- ja pääkäyttäjät).

Turvallisuuden takia osassa toimipisteistä on kameravalvonta. Valvontakamerat ja kameratallentimet tarvitsevat omat verkkoyhteytensä. Työasemille pitää asentaa ohjelmisto, jolla voi seurata valvontakameroita. Valvontaohjelmisto vaatii omat salasanansa.

Tietojärjestelmät ovat kriittinen osa päivittäistä terveystieteiden toimintaa. Ilman potilastietojärjestelmää lääkärit ja hoitohenkilökunta eivät näe ajantasaisia tietoja potilaasta (kuvio 1). Jos tietojärjestelmässä on toimintahäiriö, hoitohenkilökunta tai lääkärit eivät voi tehdä potilaasta ja potilaan hoidosta tarvittavia kirjauksia potilastietojärjestelmään. Potilasasiakirjoihin liittyvä laki määrää, että potilasasiakirjamerkinnot ovat tehtävä viivytyksettä viimeistään viiden vuorokauden kuluessa palvelutapahtuman päättymisestä (Valvira 2015, Potilasasiakirjat. Viitattu 4.4.2015). Häiriötilanteen aikana potilaiden hoito

häiriintyy; röntgenkuvat eivät siirry arkistoon, mittaustietoja, kuten spirometria tai ekg-rasitus, ei saada. Terveyskeskuksen normaalin toiminnan kannalta toimivat tietojärjestelmät ovat siis elintärkeitä.



KUVIO 1. Tietojärjestelmät ja hoitotyö.

Usealla eri paikkakunnalla toimiminen asettaa omat haasteensa tietojärjestelmille. Ne vaativat luotettavat tietoliikenneyhteydet toimiakseen. Haapavedellä sijaitsee 2013 rakennettu palvelintila, jonka tietoliikenneyhteydet operaattorille ovat kahdennettu. Palvelintilan ja palvelinten sähkönsyöttö on varmistettu ups-laitteilla, jotka ovat liitetty diesel-varavoiman taakse. Diesel-generaattorit käynnistyvät puolenminuutin sähkökatkoksen jälkeen. Terveyskeskusten ja muiden toimipisteiden verkkoyhteydet ovat toteutettu MPLS-verkkona. Etäyhteydet Helmen verkkoon on toteutettu SSL-VPN yhteydellä. Poikkeuksena

ohjelmistotoimittajien huoltoyhteydet, joita varten palomuriin on avattu omat, rajatut pääsyt kyseisten toimijoiden ilmoittamista julkisista ip-osoitteista ja tarvittavista tietoliikenneporteista.

1.3 Sote-Helmen käyttäjät

Sosiaali- ja terveystieteiden Helmessä käyttäjätunnuksia tarvitaan usealle eri tyyppiselle käyttäjälle. Koska päivystystoiminta on osittain ulkoistettu, on osa päivystävistä lääkäreistä ”käypäläisiä”, jotka saattavat käydä tekemässä päivystystä vain yhden päivän. Käypäläisille ei useinkaan ole anottu käyttäjätunnuksia valmiiksi, vaan ne pitäisi saada käyttäjälle tämän tullessa aamulla töihin. Sairaslomien ja muiden vakituisten työntekijöiden poissaolojen tilalle kutsutuilla sijaisilla käyttäjätunnusten ongelmat ovat pitkälti samat.

Toistaiseksi voimassaolevilla työsopimuksilla käyttäjätunnukset ovat voimassa, kunnes esimies ilmoittaa käyttäjän poistuneen organisaatiosta. Sekä verkko- että Efficatunnukset jäävät usein voimaan pitkäksi aikaa käyttäjä poistuessa organisaatiosta. Puhumattakaan muista käyttäjälle myönnettyistä tunnuksista lukuisiin muihin tietojärjestelmiin. Tämä on selkeä tietoturvaongelma. Osa erikoislääkäreistä käy organisaatiossa töissä vain muutaman päivän kuukaudessa. Heidän käyttäjätunnuksensa ovat voimassa samalla tavalla kuin toistaiseksi voimassa olevilla työsopimuksilla. Näissä tapauksissa salasanan unohtaminen on isoin ongelma. Ongelma korostuu, koska erikoislääkärit toimivat organisaatiossa usein kello 16:00 jälkeen.

Organisaatiossa on myös määräaikaista työsopimuksia, jolloin tunnukset ovat tehty menemään lukkoon muutama päivä ilmoitetun työsopimuksen päätyttyä. Havaintojen mukaan tässä on ongelmia, kun työsopimuksen jatkumisesta ei muisteta ilmoittaa ylläpidolle. Työsopimuksen jatkuessa käyttäjät joutuvat soittamaan ylläpitoon, kun heidän tunnukset ovat menneet lukkoon. Työharjoittelussa olevat opiskelijat vastaavat käyttäjätunnusten osalta määräaikaista työsopimuksia omaavia käyttäjiä. Myös tunnuksiin liittyvät ongelmat ovat

samat.

Kolmannet osapuolet tarvitsevat myös tunnuksia Sote-Helmen verkkoon. Esimerkiksi Tieto Efficaa ja Plandent Romexista varten tarvitsevat omat käyttäjätunnukset ja pääsyn verkkoon etäyhteydellä. Yritykset tekevät etäyhteyden kautta ohjelmistojen ylläpitoa, kuten versiopäivityksiä. Usein ohjelmisto- ja laitetoimittajien asentajat tarvitsevat myös asennustunnukset, joilla voivat asentaa Helmen työasemille laitteiden tarvitsemat ajurit ja ohjelmistot tai käyttöön hankitut uudet ohjelmat.

Käyttäjäoikeudet ovat määritelty siten, että vain ylläpidolla on toimialueen hallintatunnukset. Muut käyttäjät ovat peruskäyttäjät-ryhmässä. Heillä ei ole oikeuksia asentaa ohjelmistoja koneelle. Poikkeuksen tähän tekevät oman työnsä ohella toimivat Effica-pääkäyttäjät. Heille on annettu aktiivihakemiston Juuri-nimisestä organisatorisesta yksiköstä oikeus hallinnoida käyttäjätunnuksia. Kyseisille käyttäjille on asennettu työasemille tätä varten aktiivihakemiston käyttäjät ja ryhmät-hallintasovellus. Erityisestä syystä jotkin käyttäjät ovat saaneet työasemalle paikalliset järjestelmävalvojan oikeudet.

1.4 Tutkimusongelma

Päättötyö tutkii organisaation käyttäjätunnusten anomisprosessia ja käyttäjätunnusten hallintaa. Tavoitteena on tuoda käyttäjätunnusten anomisessa ja hallinnassa mahdollisesti esiintyvät ongelmat esille. Havaittujen ongelmien pohjalta laaditaan parannusehdotukset ongelmien korjaamiseksi ja toiminnan kehittämiseksi.

2 TOIMINTAAN VAIKUTTAVAT LAIT

Terveystoimen toimintaan vaikuttaa useat lait ja asetukset. Säädettyt lait ja asetukset vaikuttavat luonnollisesti terveyskeskuksen toimintaan, mutta myös tietojärjestelmiin ja niiden käyttäjätunnuksiin. Julkisen terveydenhuollon tietojärjestelmät ja niiden kehittäminen eroavat muiden toimialojen tietojärjestelmistä eniten juuri tämän laki-näkökohdan kautta.

2.1 Lainsäädäntö

Sosiaali- ja terveysministeriö (STM) valmistelee lainsäädäntöä ja vastaa sosiaali- ja terveystalitiikasta. Terveydenhuollon tavoite on ylläpitää ja edistää väestön terveyttä, hyvinvointia, työ ja toimintakykyä, sosiaalista turvallisuutta sekä vähentää terveyseroja. Vastuu terveydenhuollon järjestämisestä ja rahoittamisesta on kunnilla. Terveyden ja hyvinvoinnin laitos (THL) on asiantuntija- ja tutkimuslaitos. Sen tehtävänä on terveystalveluiden tutkimus ja kehittäminen sekä muut alan asiantuntijatehtävät. Sosiaali- ja terveystalan valvonta- ja lupavirasto (Valvira) valvoo, ohjaa ja hoitaa lupahallintoa sosiaali- ja terveydenhuollossa. (STM, terveystalvelut. Viitattu 7.3.2015.)

Henkilötietolaissa 523/1999 säädetään henkilörekistereistä, hyvistä henkilötietojen käsittelytavoista ja yksityisyyden suojaa turvaavista perusoikeuksista henkilötietoja käsiteltäessä. Potilasasiakirjojen käsittelystä ja asiakirjoihin sisältyvien tietojen salassapidosta säädetään laissa 785/1992 (laki potilaan asemasta ja oikeuksista). Sosiaali- ja terveysministeriön asetusta potilasasiakirjoista 298/2009 noudatetaan potilasasiakirjojen laatimisessa ja sekä niiden että muun hoitoon liittyvän materiaalin säilyttämisessä. Arkistolakia 831/1994 noudatetaan potilasasiakirjojen säilyttämisessä. Sosiaali- ja terveydenhuollon julkisten ja yksityisten sosiaali- ja terveystalveluiden asiakastietojen sähköisestä käsittelystä ja valtakunnallisista tietojärjestelmäpalveluista säädetään laissa 159/2007. Laki sisältää säädökset tietojen salassapidosta, luovutuksesta, arkistoinnista ja

asiakkaan oikeuksista saada tietoa omista asiakastiedoistaan. Laki velvoittaa kaikki julkiset toimijat liittymään kansalliseen sähköiseen potilasasiakirjojen arkistopalveluun (eArkisto). Laissa sähköisestä lääkemääräyksestä 61/2007 säädetään sähköisten lääkemääräysten käsittelystä ja potilaan tiedonsaantioikeuksista (eResepti). Kela säädetään ylläpitämään valtakunnallista reseptikeskusta ja -arkistoa. Terveystieteiden laissa 1326/2010 säädetään potilastietojen luovutuksesta ja käytöstä sairaanhoitopiirin ja sen alueella toimivien terveyskeskusten välillä. (STM, lainsäädäntö, viitattu 7.3.2015.)

Keskeinen osa hoidon laatua on potilasturvallisuus. Turvallinen hoito on vaikuttavaa ja se toteutetaan oikein ja oikeaan aikaan. Potilasturvallisuudesta ja laadunhallinnasta säädetään sosiaali- terveysministeriön asetuksessa laadunhallinnasta ja potilasturvallisuuden täytäntöönpanosta laadittavasta suunnitelmasta (341/2011). (STM, lainsäädäntö. Viitattu 4.4.2015.)

2.2 Terveystieteiden tietojärjestelmien erityispiirteet

Terveystieteiden tietojärjestelmissä käsitellään potilastietoja. Useat lait ja säännökset määrittelevät potilastietojen ja potilasasiakirjojen käsittelystä. Siksi pääsynhallinta, käyttäjätunnukset mukaan lukien, terveystieteiden järjestelmiin korostuu. Luvattoman henkilön pääsy tietojärjestelmiin tai potilastietoihin, olivatpa nämä sähköisessä tai paperisessa muodossa, rikkoisi useita eri lakeja.

Hoitosuhteen luottamuksellisuus edellyttää erityistä huolellisuutta potilastietojen käsittelyssä. Potilastiedot kuuluvat oikeudellisesti yksityiselämän suojan ydinalueeseen, jota turvaavat lakien lisäksi kansainväliset ihmisoikeussopimukset, Euroopan unionin direktiivit ja perustuslaki. Pelkkä tieto siitä, että henkilö on potilas, on salassa pidettävä tieto. Tätäkään tietoa ei saa ilmaista sivullisille ilman laissa säädettyä perustetta. Potilastietojen käsittelystä ja niiden salassapitovelvoitteista säädetään useassa eri laissa. Potilaslain sisältävät säännökset ovat terveystieteiden erityislainsäädäntöä. Potilastietoja sisältyy sekä potilaan hoitoa ja

tutkimusta dokumentoiviin potilasasiakirjoihin että potilashallinnon asiakirjoihin. Laissa yksityisestä terveydenhuollosta on lisänä vaitiolovelvollisuutta koskeva säännös, joka koskee kaikkia toimintayksikössä ja sen tiloissa toimia henkilöitä asemaan ja ammattiin katsomatta. (Sosiaali- ja terveysministeriö 2012, 15. Viitattu 17.3.2015.)

Henkilötietolakia sovelletaan käsitellessä potilastietoja, jotka on tallennettu sähköisiin henkilörekistereihin tai muihin rekistereihin, joista yksittäistä potilasta koskevat tiedot ovat vaivatta saatavissa. Viranomaisten toiminnassa syntyneitä tai tallennettuja potilastietoja koskee lisäksi julkisuuslaki. Lakia sovelletaan potilasta koskeviin tietoihin huolimatta siitä, minkälaiseen viranomaisen asiakirjaan tai mihin rekisteriin ne on tallennettu. Terveydenhuollon ammattihenkilöitä koskee ammattihenkilölaissa säädetty salassapitovelvollisuus. Edellä mainitut lait ja niiden sisältävät säädökset koskevat koulutuksesta ja asemasta riippumatta kaikkia henkilöitä, jotka osallistuvat potilaan hoitoon tai hoitoon liittyviin tehtäviin terveydenhuollon toimintayksikössä tai sen lukuun toimiessa. (Sosiaali- ja terveysministeriö 2012, 15 – 16. Viitattu 17.3.2015.)

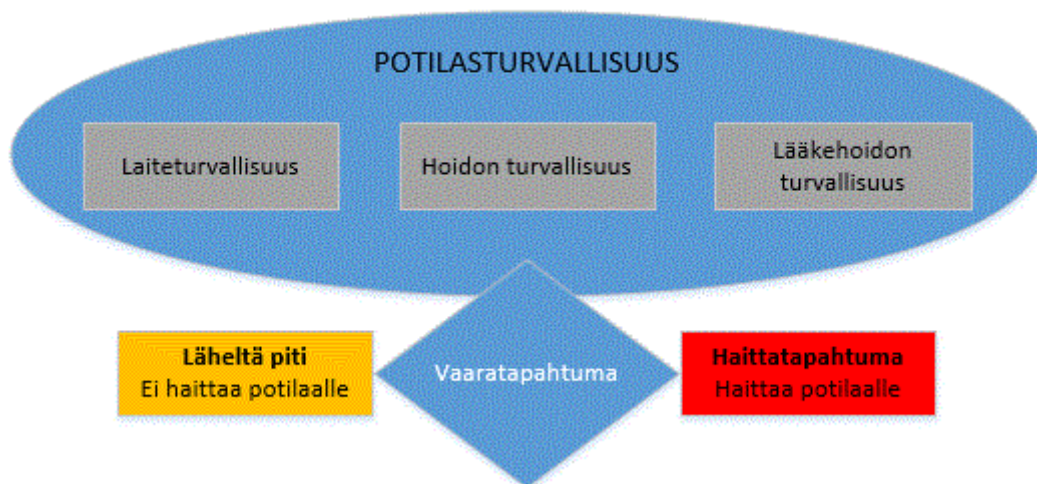
Henkilötietolain mukaan henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia koskevat tiedot ovat arkaluonteisia henkilötietoja. Arkaluonteisia henkilötietoja saa kerätä, tallentaa, käyttää ja muutoin käsitellä vain laissa säädetyin tavoin ja perustein. Henkilötietojen käsittelyä on tietojen kerääminen, tallentaminen, järjestäminen, käyttö, siirtäminen, luovuttaminen, säilyttäminen, muuttaminen, yhdistäminen, suojaaminen, poistaminen, tuhoaminen ja muut henkilötietoihin kohdistuvat toimenpiteet. (Sosiaali- ja terveysministeriö 2012, 16. Viitattu 17.3.2015.)

Tiukan tietosuojan lisäksi terveydenhuollon tietojärjestelmiin ja järjestelmien käyttöön vaikuttaa laki potilasturvallisuudesta (kuviot 2). Potilasturvallisuudella tarkoitetaan terveyshuollossa toimivien yksiköiden ja organisaatioiden periaatteita ja toimintoja, joilla varmistetaan hoidon turvallisuus ja suojataan potilasta vahingoittumiselta. Potilaan näkökulmasta potilasturvallisuus on oikeaa hoitoa, oikeaan aikaan, oikealla tavalla ja hoidosta

aiheutuu mahdollisimman pientä haittaa. Potilasturvallisuus on siis hoitoa, jossa potilaalle ei koidu vaaraa vahingon, erehdyksen, unohduksen tai lipsahduksen vuoksi. Potilasturvallisuuteen kuuluu myös hoitoyksikön periaatteet, käytännöt ja hyvät prosessit, joilla riskejä ja vaaratilanteita ennakoidaan ja estetään; inhimillisten virheiden ehkäisy estää yli puolet vahingoista. Potilasturvallisuus on jokaisen yhteinen asia, joka kuuluu jokaiselle potilasta hoitavalle. Tarkoitus on oppia yhdessä, eikä syyllistää ketään. (Terveystieteiden tutkimuskeskus, 2014. Potilasturvallisuus. Viitattu 4.4.2015.)

Potilasturvallisuuteen kuuluu kolme osa-aluetta;

1. hoidon turvallisuus (hoitomenetelmät ja hoitaminen)
2. lääkehoidon turvallisuus (lääkkeet ja lääkitys)
3. lääkinnällisten laitteiden turvallisuus (laitteiden turvallisuus ja niiden käytön turvallisuus).



KUVIO 2. Potilasturvallisuus ja vaaratapahtuma. Kuvio pohjautuu STM:n sivuilla esitettyyn kuvioon potilasturvallisuudesta.

Potilasturvallisuudessa vaaratapahtuma voi olla joko läheltä piti-tilanne tai haittatapahtuma. Läheltä piti-tilanteessa potilaalle vaarallinen turvallisuusuhka havaitaan ajoissa, jolloin potilaalle ei aiheudu haittaa. Haittatapahtumassa potilaalle aiheutuu eriasteista hoitoon kuulumatonta haittaa. (Terveyden ja hyvinvoinnin laitos, 2014. Potilasturvallisuus. Viitattu 4.4.2015.)

2.3 Sähköinen lääkemääräys (eResepti) ja sähköinen potilastiedon arkisto (eArkisto)

Kanta-palveluihin liittyvän potilastietojärjestelmän pitää tukea roolipohjaista käyttöoikeuksien hallintaa sekä käyttää vahvaa tunnistamista. Järjestelmissä pitää pystyä tunnistamaan luotettavasti henkilöt, joilla on oikeus käyttää Kanta-palveluja. Ennen liittymistä organisaatiolla tulee olla käytössä toimiva käyttöoikeuksien hallintajärjestelmä ja -menettely. Lisäksi käytössä pitää olla väestörekisterikeskuksen (VRK) myöntämät varmennekortit ja varmennepalvelu. (Kanta, liittymisohje 2013, viitattu 7.8.2014.)

Asiakastietolaki eli laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä velvoittaa julkiset terveydenhuollon organisaatiot tallentamaan potilastiedot valtakunnallisesti keskitettyyn arkistoon. Myös yksityisille terveydenhuollon organisaatioille keskitetyn arkiston käyttöönotto on pakollista, jos potilasasiakirjojen pitkäaikaissäilytys toteutetaan sähköisesti. (Kanta, lainsäädäntö 2014, viitattu 13.7.2014.)

Sähköinen potilastiedon arkisto on terveydenhuollon järjestelmä, jota käytetään potilastietojärjestelmällä. eArkisto mahdollistaa keskitetyn sähköisten potilastietojen arkistoinnin ja tietojen pitkäaikaisen säilyttämisen. Järjestelmällä on keskeinen rooli tietojen välittämisessä terveydenhuollon organisaatioiden ja toimintayksiköiden kesken. Tietojen siirtely järjestelmästä toiseen mahdollistuu, koska potilastiedot arkistoidaan teknisesti yhtenevässä muodossa. Tämä parantaa tietojen saatavuutta potilaan hoitoon osallistuvissa

toimintayksiköissä. (KanTa, potilastiedon arkisto 2014, viitattu 13.7.2014). Sosiaali- ja terveystieteiden tutkimuskeskus Helmi liittyi potilastiedon arkistoon 22.5.2014 (KanTa, arkistoa käyttävät terveydenhuollon yksiköt, viitattu 13.7.2014).

eArkisto edellyttää organisaatioilta vahvan salasanan käyttöä. Salasanan pitää olla vähintään kahdeksan merkkiä pitkä. Siinä pitää olla erikoismerkkejä, numeroita ja isoja/pieniä kirjaimia. Käyttäjän pitää vaihtaa salasana 40 päivän välein ja järjestelmän pitää muistaa ja estää edellisten 12 salasanan käyttö. (KanTa, kansalliset auditointivaatimukset 2014, viitattu 13.7.2014.)

3 SOTE-HELMEN KÄYTTÄJÄTUNNUSTEN HALLINTA

Käyttäjätunnusten hallintaan vaikuttavat tietoturvaliiketoiminta, tietoturvakäytännöt sekä tekniset toteutukset. Vastuu tunnusten hallinnasta kuuluu kaikille – myös käyttäjälle itselleen. Esimiesten rooli ja vastuu on tunnusten ja tarvittavien oikeuksien anomisessa. Ylläpito vastaa teknisestä toteutuksesta ja omalta osaltaan tunnusten luonnista ja ylläpidosta.

3.1 Helmen tekniset ratkaisut

Haapaveden kaupungilla on noin 900 ylläpidettävää työasemaa, noin 50 palvelinta ja hallittavaa kytkintä. Kriittisimmät palvelimet ja kaikki kytkimet ovat avoimeen lähdekoodiin perustuvassa Zabbix-valvontajärjestelmässä. Valvontajärjestelmä seuraa ja hälyttää muun muassa palvelimien prosessorikuorman, keskusmuistin tai kovalevytilan ylittäessä annettu hälytysraja. Kytkinverkosta valvotaan pingillä kytkinten ylhäällä oloa. Palomuurista seurataan liitännöiden tilaa, avoimia yhteyksiä ja kaistan käyttöä. Zabbix-valvonta on toteutettu yhteistyössä Kalajoen kaupungin kanssa. Verkkoyhteydet ovat kriittiset, koska potilastietojärjestelmä toimii verkon päällä; verkkovian sattuessa käyttäjät eivät pääse potilastietojärjestelmään.

Siikalatvan ja Haapaveden vuodeosastoilla sekä Haapaveden terveyskeskuksen aulassa ja hallinnon tiloissa on kontrolleri-pohjainen langatonverkko, jonka tuotantoverkkoon pääsee vain toimialueeseen liitetyt koneet. Langattoman verkon tukiasemat kaiuttavat myös avointa vierailijaverkkoa, johon käyttäjä pääsee hyväksymällä käyttäjäehdot. Vuodeosastoilla langatonta verkkoa tarvitsevat lääkäri ja osastonhoitaja päivittäisellä lääkärikierrolla.

Työasemat jakaantuvat siten, että Sote-Helmessä on noin 320 työasemaa, sivistyspuolella noin 290 ja loput koneet hallinnossa, sosiaalitoimessa ja muissa hallintokunnissa. Sote-Helmessä

on vielä 3 Windows XP-käyttöjärjestelmällä varustettua työasemaa, jotka poistuvat EKG- ja spirometrialaitteiden uusimisen kautta. Palvelimista yhdeksän on fyysisiä palvelinrautoja. Näiden lisäksi löytyy neljä fyysistä virtuaalipalvelinrautaa, joissa loput palvelimet pyörivät virtuaalisina. Kolmen virtuaalipalvelimen klusteri on kiinni levytallennusjärjestelmässä.

3.2 Käyttäjätunnusten hallinnointi

IT-tiimiin kuuluu neljä henkilöä; it-päällikkö, kaksi it-suunnittelijaa sekä Effica-pääkäyttäjä. Lisäksi organisaatiossa on kaksi oman työnsä ohella olevaa Effica-pääkäyttäjää. Vaikka it-tiimissä vastuualueet on jaettu tarkasti, joutuu käytännössä jokainen tekemään kaikkea. Sote-Helmen Windows 7-käyttöjärjestelmällä varustettujen työasemien paikoilleen asennus ulkoistettiin Tietolatva Oy:lle resurssipulan vuoksi.

Käyttäjätunnuksia luo ja hallinnoi useat eri ihmiset. Lähes jokaiseen käytössä olevaan järjestelmään on käyttäjillä omat tunnukset ja salasanat. Taulukkoon 1 on kerätty ja listattu yleisimmät järjestelmät ja kenelle niiden salasanojen hallinta kuuluu. Myöhemmin kuviossa neljä on havainnollistettu alla oleva taulukko kuviona.

TAULUKKO 1. Sote-Helmessä käytössä olevia tietojärjestelmiä ja niiden käyttäjätunnusten hallintavastuu.

JÄRJESTELMÄ	YLLÄPITÄJÄ
verkkotunnukset	It-tiimi ja Effica-pääkäyttäjät
sähköposti	it-tiimi
Effica	Effica-pääkäyttäjät
ePopulus	palkanlaskijat
Web-tallennus	palkanlaskijat
NeaRIS	röntgenhoitajat
Effector	nimetyt pääkäyttäjät
TeleQ	esimiehet
Dynasty	hallintojohtaja, tietopalvelusihteeri
Titania	atk-päällikkö
Eemeli	Oys?
Romexis	pääsy rajattu aktiivihakemiston ryhmällä
Spiro	pääsy rajattu aktiivihakemiston ryhmällä
Kameravalvonta	Kameravalvonnan toimittaja?
Navisec	kaksi esimiestä ja tietoturvavastaava

Yllä olevista järjestelmistä sähköposti olisi mahdollista integroida AD-tunnuksiin. Effector on integroitu AD:hen, joten käyttäjä voi kirjautua siihen omilla verkkotunnuksillaan. Näin vältetään yksiltä uusilta käyttäjätunnuksilta ja salasanoilta. Potilastietojärjestelmään (Effica) tämä ominaisuus on tulossa todennäköisesti vuoden 2016 aikana. Asiasta on keskusteltu toimittajan eli Tieto Oyj:n kanssa viimeksi Tampereella Tieto Oy:n järjestämässä pääkäyttäjäforumilla.

3.3 Nykyinen tunnusten anomisprosessi

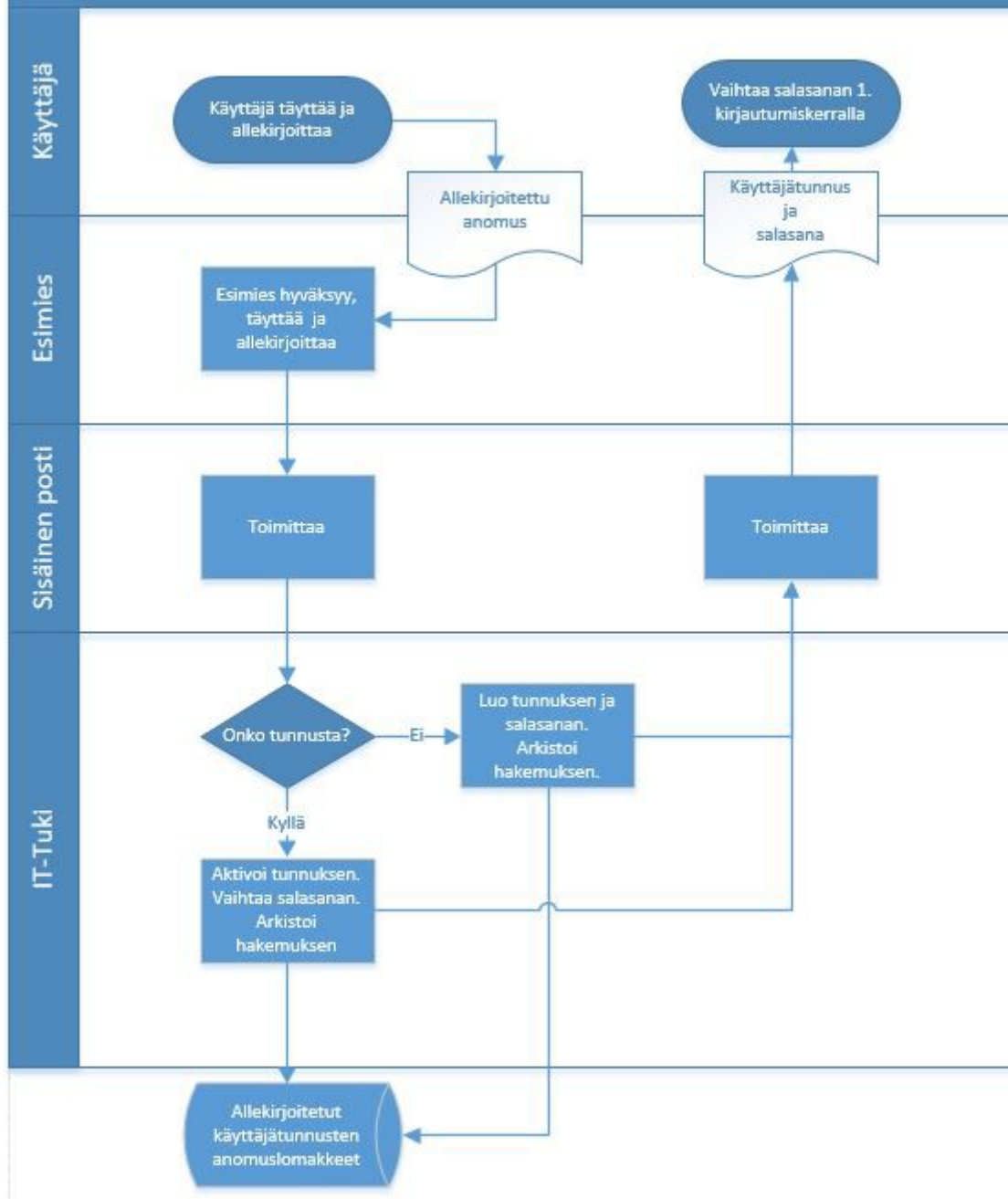
Nykyisen prosessin mukaan esimies täyttää intranetistä löytyvän sähköisen käyttäjätunnusten anomislomakkeen (liite 1). Lomakkeeseen merkitään ne järjestelmät, joihin käyttäjän täytyy

saada tunnukset. Samalla esimies tulostaa käyttäjälle salassapitosopimuksen (liite 2). Jos ja kun käyttäjä tarvitsee tunnukset myös Efficaan, tulostaa esimies tähän erikseen tarkoitettua anomislomakkeen (liite 3). Efficalle on erillinen tunnustenanomislomake siksi, että terveydenhuollon tietojärjestelmät vaativat käyttäjältä enemmän tietoja. Näitä ovat muun muassa Terhikki-rekisterinumero ja sosiaaliturvatunnus.

Terveydenhuollon ammattihenkilöiden keskusrekisteri Terhikki on Valviran ylläpitämä julkinen tietopalvelu. Rekisteri perustuu terveydenhuollon ammattihenkilöistä annettuun lakiin ja asetuksiin. Tietopalvelusta voi tarkistaa ammattihenkilön ammattipätevyyden. Tiedot päivitetään kerran vuorokaudessa. Terveydenhuollossa on sekä laillistettuja että nimikesuojattuja ammattihenkilöitä. Kaikki nimikesuojatut ammattihenkilöt eivät välttämättä tarvitse Valviran hyväksyntää ammattinimikkeen käyttöön. Oikeus käyttää suojattua ammattinimikettä tulee heille suoraan koulutuksen perusteella. Tällaisia ovat esimerkiksi lähihoitajat. Heistä kaikki eivät ole ilmoittaneet tietojaan Valviran rekisteriin, mutta ovat siitä huolimatta terveydenhuollon ammattihenkilöitä. (Valvira, terveydenhuollon ammattihenkilö 2015. Viitattu 28.3.2015.)

Sekä esimies että käyttäjä allekirjoittavat tulostetut ja täytetyt lomakkeet, jotka sitten postitetaan organisaation sisäisellä postilla ylläpidolle. Kirjeen saatuaan ylläpito luo lomakkeessa pyydetyt tunnukset, tulostaa tunnustenluovuttamista varten tehdyn lomakkeen (liite 4) ja postittaa sen sisäisessä postissa käyttäjälle (kuva 3).

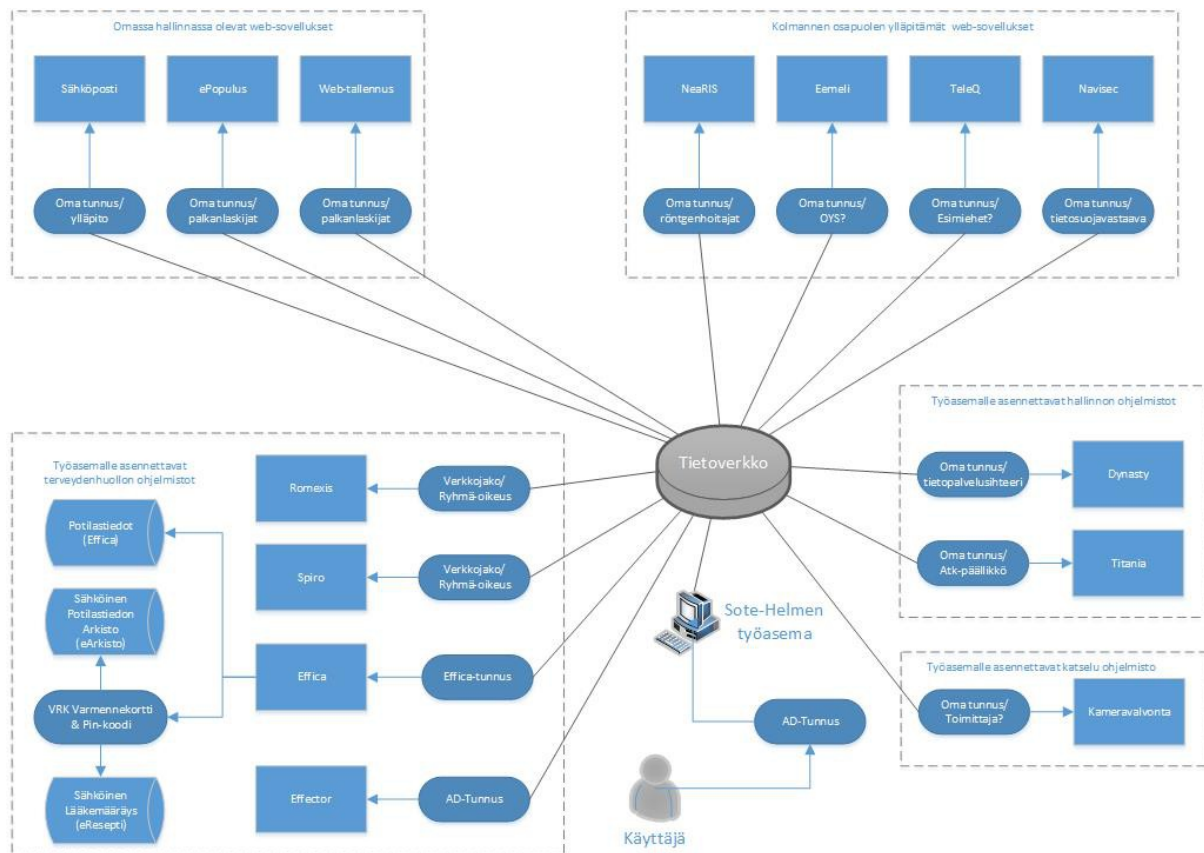
Käyttäjätunnuksen anominen



KUVIO 3. Prosessimalli käyttäjätunnusten anomisprosessista.

3.4 Käyttäjän todentaminen

Tietojärjestelmän pitää pystyä erottamaan oikea käyttäjä väärästä. Käyttäjä todennetaan yleisesti joko salasanalla tai pin-koodilla. Pin-koodit ovat hankalia, koska käyttäjä ei voi useinkaan niitä valita. Pelkkinä numeroina pin-koodit ovat myös hankalia muistaa. Vaikka salasana olisikin niin sanottu vahva salasana, on siinä silti heikkouksia. Käyttäjä voi unohtaa salasanansa aivan, kuten käyttäjä voi hukata avaimensa tai varmennekorttinsa. Salasana voidaan luovuttaa myös kolmannelle osapuolelle puhelimesta tai sähköpostilla. Joku voi saada salasanan haltuunsa oman yli katsomalla, kokeilemalla eri vaihtoehtoja tai löytämällä muistilapun. Ongelmana on se, ettei salasanan vuotamista välttämättä huomata helposti. Tunkeutuja voi pahimmillaan sulkea oikean käyttäjän pois järjestelmästä vaihtamalla salasanan. (Järvinen 2012, 112 – 113.)



KUVIO 4. Ohjelmistot ja käyttäjätunnukset.

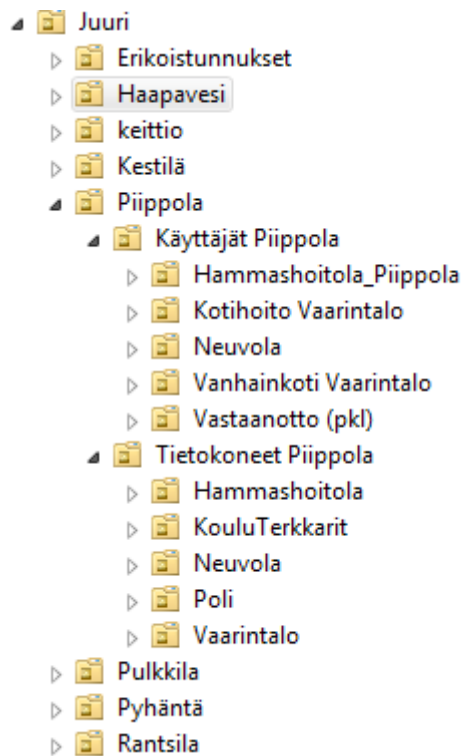
Sosiaali- ja terveystieteiden Helmessä on käytössä lukuisia salasanoja eri järjestelmiin sekä henkilövarmennekortit, jotka eResepti ja eArkisto vaatii. Varmennekorteja varten lähes jokaisella työasemalla on asennettu kortinlukijanäppäimistö ja tunnistautumiseen tarvittavat ohjelmistot. Salasanoja unohdetaan tasaisin väliajoin – varsinkin pidempien lomien jäljiltä. Vastaan on tullut myös tapauksia, joissa käyttäjätunnus ja salasana ovat näppäimistöllä/työpöydällä näkyvissä lapulla. Näissä tapauksissa käyttäjä on yleensä joutunut esimiehen puhutteluun. Ehdottomasti kriittisimmät salasanat ovat verkkotunnukset ja Efficatunnukset. Efficat sisältää potilastiedot ja verkkotunnuksilla käyttäjä pääsee kirjautumaan organisaation koneille, saa pääsyn sisäverkkoon ja verkkolevyihin. Yllä olevassa kuviossa (kuvio 4) on visualisoitu käyttäjien tunnusviidakkoa eri järjestelmiin. Kuvio löytyy isompana

päättötyön lopusta liitteenä (liite 5).

3.5 Active Directory

Aktiivi hakemiston (AD) kautta hallitaan käyttäjä, ryhmä ja tietokone-objekteja. Objekti sisältää tietoa, kuten objektin kuvauksen, käyttöoikeudet, sovellusoikeudet. AD:n ”Users and Computers” kautta voidaan luoda, muokata ja poistaa objekteja hakemistosta. Hakemistopuussa objektit eivät ole yleensä yhdessä isossa ryhmässä vaan ovat lajiteltu organisatorisiin yksiköihin. Nämä usein sisältävät toisia organisatorisia yksiköitä. Näin hakemistosta muodostuu puumainen rakenne, jossa organisatoriset yksiköt ovat puun runko ja objektit lehtiä. Usein aktiivihakemiston rakenne peilaa yrityksen todellista rakennetta. Esimerkiksi eri toimipisteet saavat omat organisaatioyksiköt (organization unit, OU) hakemistoon, joiden alle luodaan käyttäjät ja tietokonetilit. Aktiivi hakemiston ”Users and Computers” yleisimpiä tehtäviä ovat käyttäjätilien luonti, salasanojen vaihto, oikeuksien asettaminen levyjakoihin ja käynnistyskriptien asettaminen. (TechRepublic Windows Server 2008 2008, viitattu 7.8.2014.)

Haapaveden kaupungin aktiivi hakemiston rakenne Sote-Helmen osalta on jaettu ylähakemistoon (Juuri), joka on jaettu paikkakunnittain. Jokaisella paikkakunnalla on erikseen hakemistot tietokone- ja käyttäjätileille. Nämä on puolestaan jaettu vielä osastoittain tai toimipaikoittain, kuten poli, labra, vuodeosasto jne. NordLabille ja Tietolatvalle on tehty aktiivihakemistopuun juureen omat organisatoriset yksiköt. Alla oleva kuvio (kuvio 5) näyttää, miten Sote-Helmen aktiivihakemiston puu on rakennettu.



KUVIO 5. Ruudunkaappaus Sote-Helmen aktiivihakemiston hakemistopuusta.

3.6 Kertakirjautuminen

Enterprise Single Sign On eli eSSO tarkoittaa kertakirjautumista. Erilaiset työasemassa ajettavat sovellukset kytketään kertakirjautumisen piiriin. Työasemille asennetaan ohjelmisto, joka on yhteydessä keskitetyssä käyttäjähakemistossa sijaitsevaan kertakirjautumistietoon ja sovellusmäärittelyihin. Käyttäjän kirjautuessa työasemalle ja verkkoon, kertakirjautumisohjelmisto saa tiedon siitä, kuka koneella on ja mitkä sovellukset on määriteltä kertakirjautumisen kohteeksi. Sovellusohjelman havaitessa kertakirjautumisen

piiriin kuuluvan sovelluksen käynnistymisen, syöttää ohjelmisto automaattisesti vaadittavat kirjautumistiedot sovellusohjelmistoon ja päästää käyttäjän sovellukseen ilman käyttäjän havaitsevaa kirjautumisprosessia. (Kertakirjautuminen, viitattu 24.10.2014.)

4 TUTKIMUS JA TULOKSET

Kehittämistyössä on mahdollista ja suositeltavaa käyttää useita menetelmiä. Laadullisen tutkimuksen tyypillisiä menetelmiä ovat teema-, avoin ja ryhmähaastattelu sekä osallistuva havainnointi. Tarkoituksena on hankkia suppeasta kohteesta paljon tietoa. Näin tutkittavaa ilmiötä voi ymmärtää paremmin ja kokonaisvaltaisemmin. Laadullisen tutkimuksen lähtökohtana on todellisen elämän kuvaaminen. Todellisuus ymmärretään moninaisena kokonaisuutena, jota ei voi jakaa mielivaltaisesti osiin. Tutkimuksen kohde on harkitusti valittu. Tutkimusprosessin tarkka kuvaus ja tulkintojen perustelut ovat tärkeitä, koska niiden avulla lukija voi tehdä päätelmiä tutkimuksen luotettavuudesta. (Ojasalo & Moilanen & Ritalahti 2009, 93 – 94.)

Koska päättötyön tekijä työskentelee itse organisaatiossa, on hyvin luontevaa valita havainnointi tutkimusmenetelmäksi. Tätä täydentää hyvin esimiehille tehtävä kyselytutkimus, joka kartoittaa ongelmaa toisesta näkökulmasta. Omien havaintojen tukena toimivat myös työkavereiden kanssa käydyt keskustelut käyttäjätunnuksista ja niihin liittyvistä ongelmista. Koska keskustelua on käyty useita kahden ja puolen vuoden aikana, eikä niitä ole kirjattu ylös, varmistettiin keskustelujen johtopäätöksiä tekemällä it-tiimille ja Effic-pääkäyttäjille suppea kyselytutkimus.

4.1 Tutkimuksen teko

Yhdeksälletoista sosiaali- ja terveystyöntekijälle Helmen esimiehelle lähetettiin sähköpostilla linkki internetissä täytettävään Webropol-kyselylomakkeeseen. Kyselylomakkeen kysymykset ovat tämän päättötyön liitteenä (liite 6). Kyselyllä pyrittiin selvittämään, miten esimiehet hahmottavat ja kokevat nykyisen käyttäjätunnuksien anomisprosessin. Samalla selvitettiin, kokevatko esimiehet käyttäjätunnuksien anomisessa tai hallinnassa olevan ongelmia ja mitä nämä mahdolliset ongelmat ovat. Kyselyssä ei selvitetä vastaajien taustoja, kuten osastoa tai

tiimiä, koska vastausjoukko on hyvin rajattu. Käytännössä jo vastaajan tiimistä pystyisi päättämään vastaajan henkilöllisyyden. Kysely lähetettiin vain esimiehille siksi, että he ovat keskiössä käyttäjätunnuksia anottaessa ja hallinnoidessa.

IT-tiimin jäseniä sekä Effican pääkäyttäjiä haastateltiin työn ohessa lisätiedon saamiseksi. Varsinaista kyselykaavaketta ei ollut, vaan asiaa käsiteltiin työn ohessa, tauoilla ja palavereissa ”rupatteleamalla”. Heille lähetettiin vielä hyvin suppea kysely (liite 7) keskustelujen johtopäätösten varmistamiseksi. Koska virallista kyselylomaketta ei ole käytetty, on osa keskustelujen johtopäätöksistä ja anneista käsitelty omissa havainnoissa. Apuna käytettiin siis myös omia havaintoja, jotka kirjattiin havainnointipäiväkirjaan ylös.

4.2 Kyselytutkimus esimiehille

Kyselytutkimusten etuna on se, että niiden avulla voidaan kerätä laaja tutkimusaineisto, jossa suurelta määrältä ihmisiä voidaan kysyä useita asioita. Menetelmä on nopea ja tehokas. Kyselyt tuottavat paljon numeroihin perustuvia tuloksia, joita voidaan käsitellä tilastollisesti. Kyselyn heikkoutena pidetään tuotetun tiedon pinnallisuutta sekä sitä, ettei pystytä arvioimaan, miten vakavasti vastaaja on suhtautunut tutkimukseen tai miten onnistuneita annetut vastausvaihtoehdot ovat vastaajan näkökulmasta. Heikkoutena on myös se, ettei tiedetä, miten tietoisia vastaajat ovat tutkimusaiheesta tai miten perehtyneitä he siihen ovat. Kysely soveltuu hyvin useiden aiheiden ja ilmiöiden tutkimukseen. Kyselytutkimusta suunniteltaessa on muistettava, että se on määrällisen tutkimuksen menetelmä. Kvantitatiivinen tutkimus pyrkii kuvailemaan ja selittämään tutkimuksen kohteena olevaa ilmiötä järjestelmällisten havaintojen avulla. (Ojasalo & Moilanen & Ritalahti 2009, 108 – 109.)

Koska tutkimukseen osallistuvien henkilöiden lukumäärä on rajattu kohtuullisen suuruiseksi, tehdään kysely koko perusjoukolle, jolloin kyselyn otanta on 100%. Linkki Webropol-kyselyyn lähetettiin sähköpostilla 19 esimiehelle. Kysely oli avoinna 7.4 – 17.4.2015 ja siinä

ajassa kyselyyn vastasi 6 henkilöä. Vastausprosentiksi muodostui 31,6%. Koska vastausten määrä jäi alhaiseksi, on tuloksista hankala vetää varmuudella isompia johtopäätöksiä. Vastausmäärä peilaa oman havainnon mukaan hyvin it-puolen ja esimiesten/työntekijöiden välistä suhdetta. Usein tietotekniikka koetaan työtä haittaavaksi tai hankaloittavaksi tekijäksi, eikä tietotekniikkaa ole integroitu osaksi työn luonnollista suorittamista. Näin ei tietotekniikasta saada maksimaalista hyötyä irti. Vastausten määrästä voi vetää johtopäätöksen, ettei tietotekniikka kiinnosta – ellei ole pakko. Koska tietotekniikka on arjen työstä irrallaan oleva osio, on muodostunut raja-aitoja ja näkymättömiä esteitä kenttäväen ja it-puolen välille.

Kyselyssä oli kaksi kohtaa, joissa vastaajaa pyydettiin arvioimaan väittämiä kouluarvosanoilla; 1 huono, 2 välttävä, 3 tyydyttävä, 4, hyvä, 5 kiitettävä. Ensimmäinen väittämäpatteri liittyi käyttäjätunnusten anomisprosessiin, toinen käyttäjätunnusten hallintaan (taulukko 1 ja taulukko 2).

TAULUKKO 2. Väittämäkysymykset liittyen käyttäjätunnuksien anomiseen.

	1	2	3	4	5	Yhteensä	Keskiarvo
Ohjeistus tunnusten anomiseen on helposti löydettävissä.	0	1	3	1	1	6	3,33
Ohjeet tunnusten anomiseen ovat selkeät.	0	2	1	2	1	6	3,33
Nykyinen tunnusten anomisprosessi toimii sujuvasti.	1	3	0	1	1	6	2,67
Anomisprosessi on joustava.	1	2	0	1	2	6	3,17
Saan tarvittavat käyttäjätunnukset nopeasti.	1	3	0	1	1	6	2,67
Saan kerralla käyttäjätunnuksiin liittyvät asiat kuntoon.	0	2	3	0	1	6	3
Käyttäjätunnusten anomislomake on helppo täyttää.	0	1	2	2	1	6	3,5
Tarvittaessa saan apua ylläpidolta nopeasti.	0	0	1	3	2	6	4,17
Ylläpito tukee tarpeeksi.	0	0	1	3	2	6	4,17
Täytän käyttäjätunnuksien anomislomakkeen valmiiksi työsopimuksen teon yhteydessä.	0	1	2	1	2	6	3,67
Nykyinen paperinen tunnusten anomisprosessi on riittävä.	2	1	2	0	1	6	2,5
Yhteensä	5	16	15	15	15	66	3,29

Vastauksista huomioitavaa tulokset, jotka jäivät alle kolmen keskiarvon. Näitä ovat anomisprosessin sujuvuus, käyttäjätunnusten nopea saanti ja nykyisen anomisprosessin riittävyys. Vastauksen kertovat, että nykyinen anomisprosessi paperisella lomakkeella ja sisäisellä postilla on liian hidas. Tämä puoltaa anomisprosessin muuttamista sähköiseen muotoon. Omat havainnot tukevat tätä tulosta.

Tuloksissa reilusti yli kolmen keskiarvolle kohosivat kysymykset koskien ylläpitoa. Esimiehet kokivat saavansa it-tuelta tarvittavan avun ja saavansa avun nopeasti. Keskiarvo 4,17 on erittäin hyvä tulos! Käyttäjätunnusten anomislomake koettiin myös kohtuullisen helpoksi

täyttää (3,5). Esimiehet vastasivat myös täyttävänsä käyttäjätunnusten anomislomakkeen työsopimuksen teon yhteydessä. Tämä on osittain ristiriidassa omien havaintojen kanssa. Ristiriitaa selittänee vastausten määrä.

Vastausten valossa käyttäjätunnusten anomisen ohjeistusta voisi tarkistaa, vaikei siinä koettukaan mitään suuria ongelmia. Anomisprosessin joustavuutta voisi koittaa myös parantaa. Tätä tukee se, että väittämät käyttäjätunnuksen anomiseen liittyvien asioiden kerralla kuntoon saamisesta sai keskiarvoksi tasan kolme. Pienellä vastausten määrällä yksi annettu arvosana viisi nosti keskiarvoa hämäävän paljon (2,6 → 3).

TAULUKKO 3. Väittämäkysymykset liittyen käyttäjätunnusten hallintaan.

	1	2	3	4	5	Yhteensä	Keskiarvo
Unohtuneen salasanan vaihtaminen on helppoa.	0	0	5	1	0	6	3,17
Lukitun käyttäjätunnuksen aukaisu on helppoa.	0	0	5	1	0	6	3,17
Käyttäjät unohtavat salasansansa harvoin.	3	3	0	0	0	6	1,5
Salasanoja ei ole liikaa eri järjestelmiin.	2	3	1	0	0	6	1,83
Ohjeistus käyttäjätunnusten hallintaan on riittävä.	0	0	4	1	1	6	3,5
Käyttäjätunnuksiin liittyvä ohjeistus on helposti saatavilla.	0	1	3	1	1	6	3,33
Kaupungin tietoturvapoliittikka on ajantasalla.	0	0	2	3	1	6	3,83
Käyttäjille tarkoitettu tietoturvataulu on näkyvillä.	1	1	2	2	0	6	2,83
Saan tarvittaessa apua ylläpidolta.	0	0	1	1	4	6	4,5
Saan tarvittaessa apua ylläpidolta nopeasti.	0	0	1	2	3	6	4,33
Käyttäjän poistuessa organisaation palveluksesta kaikki hänen käyttäjätunnuksensa tulee poistettua.	0	1	5	0	0	6	2,83
Ilmoitan käyttäjän poistumisesta organisaation palveluksesta ylläpidolle.	0	1	1	4	0	6	3,5
Muutoksenhaku käyttäjätunnuksiin on helppoa.	0	1	5	0	0	6	2,83
Muutoksen haku käyttäjätunnuksiin on ohjeistettu hyvin.	0	2	3	0	1	6	3
Käyttäjät ymmärtävät, mitä riskejä käyttäjätunnuksen ja salasanan joutumisesta vieraisiin käsiin liittyy.	0	0	2	2	2	6	4
Käyttäjät ovat sitoutuneita noudattamaan tietoturvapoliittikkaa.	0	0	2	4	0	6	3,67
Käyttäjät muistavat lukita tietokoneen poistuessaan työasemalta.	0	2	2	2	0	6	3
Käyttäjätunnuksia ja salasanoja ei ole kirjoitettu (muisti)lapuille työasemaan viereen näkyville (tai näppäimistön alle).	0	1	1	3	1	6	3,67
Yhteensä	6	16	45	27	14	108	3,25

Käyttäjätunnusten hallinnassa selvästi alle kolmen keskiarvon jäi viisi väittämää. Näistä eivät yllättäneet käyttäjien salasanojen unohtelu, turhan paljon salasanoina eri järjestelmiin, käyttäjän tietoturvataulun puuttuminen näkyviltä sekä käyttäjätunnusten poistoon ja hallintaan liittyvät ongelmat. Nämä vastaukset tukevat omia havaintoja. Varsinkin käyttäjien salasanojen unohtelu ja salasanojen määrä koettiin hyvin selvästi ongelmaksi. Vaikka tunnusten hallinta saikin kohtuullisen keskiarvon useammasta aiheeseen liittyvästä väittämästä, on asiaan syytä kiinnittää enemmän huomiota. Tulosten valossa käyttäjätunnusten hallintaa tulee kehittää. Käyttäjätunnusten hallinnan ohjeistusta tulee kehittää. Vaikka väittäjä sai keskiarvoksi tasan kolme, nosti yksi vastaus keskiarvoa suhteettoman paljon (2,6 → 3).

Huomattavasti yli kolmen keskiarvolle pääsivät vastaukset liittyen kysymyksiin ylläpidosta ja itselle hieman yllättäen käyttäjien hahmottaminen riskeistä liittyen käyttäjätunnuksen ja salasanan joutumisesta vieraisiin käsiin. Esimiesten vastausten perusteella ylläpito antaa apua (4,5) ja antaa apua nopeasti (4,3). Tulokset ovat erittäin hyviä, kun ottaa huomioon it-tuessa vallitsevan resurssipulan.

Vastausten perusteella tietoturta on kohtuullisessa kunnossa, vaikkei käyttäjän tietoturvataulu olekaan selkeästi näkyvillä. Tämä puute on onneksi helppo korjata. Oman havaintona tietoturvataulu pitää päivittää. Oman havainnon ja kyselyn tuloksen mukaan organisaatiosta poistuvan käyttäjän tunnusten poistoon pitää tulevaisuudessa kiinnittää nykyistä enemmän huomiota. Tietoturvan kannalta oli ilahduttavaa huomata, ettei esimiehet ole havainneet käyttäjätunnuksia kirjoitettuna paperille työaseman välittömässä läheisyydessä. Oman havaintona tällaiseen tapauksiin on törmätty puolenkymmentä kertaa ja tapauksiin on puututtu heti. Yleisesti kaupungin tietoturvapoliittikka koettiin olevan ajan tasalla (3,83), mutta tämä ei ole linjassa omien havaintojen kanssa. Esimerkiksi kaupungin tietoturvapoliittikka on päivitetty viimeksi vuonna 2008. Vastauksissa esiintyi paljon hajontaa väittämän kohdalla, että käyttäjä lukitsee tietokoneen poistuessaan työasemalta. Keskiarvoksi muodostui tasan kolme, mutta kaksi vastaajaa antoi arvosanaksi kaksi ja kaksi vastaajaa

arvosanaksi 4. Omien havaintojen mukaan tämä kuvaa vallitsevaa tilannetta hyvin. Osassa organisaatiota asia toimii ongelmitta, mutta osassa organisaatiosta käyttäjät unohtavat lukita tietokoneen poistuessaan työasemalta systemaattisesti.

Esimiehet vastasivat ilmoittavan ylläpidolle, kun käyttäjä poistuu organisaation palveluksesta (3,5). Omat havainnot eivät tätä tulosta tue. Tätä väittämän tulosta ei tue myöskään käyttäjälistan läpikäynti, jonka yhteydessä organisaatiosta poistuneiden käyttäjien tunnukset lukitaan. Selittäväenä tekijänä tässä varmastikin on kyselyyn vastanneiden määrä; osa esimiehistä hoitavat tunnusasiat esimerkiksi. Epäilen juuri näiden vastuuntuntoisten myös vastanneen kyselyyn.

Kyselyssä esimiehille esitettiin väittämien lisäksi 11 avointa kysymystä. Kuusi kysymystä liittyi käyttäjätunnusten anomiseen ja viisi liittyi käyttäjätunnusten hallintaan. Lisäksi kumpaankin aihepiiriin liittyen oli esimiehillä lopussa mahdollisuus vapaaseen sanaan. Vastausten ja tulosten syvällisempää analysointia vaikeuttaa alhainen vastausten määrä.

4.2.1 Käyttäjätunnusten anomiseen liittyvät kysymykset

Kuvaile lyhyesti nykyinen virallinen käyttäjätunnusten anomisprosessi.

Tällä kysymyksellä pyrittiin kartoittamaan, miten esimiehet hahmottavat nykyisen anomisprosessin. Käytännössä testattiin esimiesten tietämystä olemassa olevasta prosessista. Kysymykseen siis oli olemassa ”oikea vastaus”, koska tunnusten anomiselle on olemassa virallinen prosessi ja viralliset ohjeet. Kuudesta vastauksessa ainoastaan yhdessä oli maininta käyttäjätunnusten teon yhteydessä salassapitosopimuksesta. Tietyissä mielessä tämä on huolestuttava havainto – muistaako siis kukaan tehdä salassapitosopimusta? Positiivisena asiana vastauksista nousi esille kommentti: ”...järjestely on hyvä että asiakkaalle voi sanoa ettei kukaan voi katsella tietoja jos ei niitä tarvitse”.

Miten nykyinen käyttäjätunnusten anomisprosessi mielestäsi toimii?

Kysymyksellä pyrittiin selvittämään prosessin toimivuutta esimiesten näkökulmasta. Vastaukset eivät olleet yllättäviä, vaan prosessin todettiin olevan hidas, kankea ja tunnusten käyttöönoton venyvän. Prosessia pidettiin sekavana eikä aina oikein tiedetty, mitä lomakkeessa kysytään. Ongelmaksi koettiin myös se, että kaupungilla vaihtuvat jatkuvasti henkilöt, jolle lomakkeet lähetetään. Tästä on oma havainto, että käyttäjät todellakin lähettävät lomakkeet tietyille henkilöille. Tämä on erittäin huono menettelytapa, koska kyseinen käyttäjä voi olla pitkäänkin poissa töistä loman tai sairausloman takia. Tällöin nimetyt kirjeet odottavat henkilöä postilokerikossa.

Mitkä ovat nykyisen prosessin hyvät/huonot puolet?

Tällä pyrittiin löytämään prosessissa esiintyviä epäkohtia ja vahvuuksia. Vastauksissa it-päällikköä Eero Härmää keuhuttiin, että häneltä saa aina avun ja että hän aina vastaa puhelimeen. Vastaus on johdonmukainen ylläpidon saamien hyvien keskiarvojen kanssa. Sisäisen valvonnan kannalta prosessia pidettiin hyvänä. Huonona puolena mainittiin systeemin hitaus, kankeus ja vanhanaikaisuus. Erityisesti hitaus ja kankeus korostui useassa vastauksessa. Sijaiselle on hankala saada tunnukset oikeaan toimipisteeseen.

Pitäisikö nykyistä prosessia mielestäsi kehittää? Jos kyllä, niin miten?

Kysymyksellä yritettiin sekä aktivoida esimiehiä osallistumaan prosessin kehittämiseen että kalastella hyviä ja uusia ideoita. Suurimmassa osassa vastauksissa prosessia toivottiin sähköiseksi. Ehdotettiin sekä täytettävää web-lomaketta että web-tallennukseen integroitavaa lomaketta. Vastauksissa toivottiin myös esimiehille mahdollisuutta hallita käyttäjätunnuksia, kuten tarkistaa ja tarvittaessa jatkaa tunnusten voimassaoloaikaa tai vaihtaa salasana. Kehittämistarpeena nousi esille myös unohtuneet tai toimimattomat tunnukset, jotka pitäisi pystyä samaan toimintaan myös viikonloppuisin. Oli ilahduttavaa huomata, että ainakin osa esimiehistä haluaisi osallistua käyttäjätunnusten hallintaan!

Vastaako nykyinen prosessi teidän tarpeita vai puuttuuko siitä kenties jotain?

Tälläkin kysymyksellä pyrittiin nostamaan esille mahdollisia ongelmia ja toisaalta käyttäjien – siis esimiesten – tarpeita prosessille. Koska kysymys on edellisen kanssa saman luontoinen, osa esimiehistä antoi kattavan vastauksen jo edelliseen kysymykseen. Prosessi koettiin monimutkaiseksi, eikä millään muistanut, kuka mistäkin alueesta vastaa. Omien työntekijöidensä tunnusten voimassaoloaikojen näkemistä toivottiin. Puutteeksi koettiin myös se, ettei mistään näe, mitä tunnuksia kenelläkin on. Samoin esitettiin ajatusta salasanojen ja tunnusten vaihtoon hyödyntäen pankki-tunnistautumista.

Onko sinulla ollut ongelmia käyttäjätunnusten anomiseen liittyen? Jos on, niin minkälaisia?

Tällä kysymyksellä pyrittiin selvittämään esimiesten kohtaamia ongelmia tunnusten kanssa käytännön arjessa. Isommalla vastausmäärällä olisi voinut vetää johtopäätöksiä järjestelmän tilastakin. Olisi ollut hälyttävää, jos suurin osa esimiehistä olisi valittanut kohtaavansa ongelmia tunnusten anomiseen liittyen. Kokonaisuudenhallinta koettiin ongelmaksi, koska tietoa siitä, kenellä on tunnukset mihinkin, ei ole. Anomislomakkeita toivottiin selkeämmiksi. Prosessia moitittiin kankeaksi ja hitaaksi, mikä on useassa kysymyksessä esille nouseva asia. Positiivisesti yksi kolmasosa vastaajista ilmoitti, ettei ole kokenut ongelmia käyttäjätunnusten anomisessa. Vuorotyö aiheuttaa ongelmia, koska kaikki käyttäjät eivät ole aina paikalla kuulemassa ohjeistusta. Organisaatioon on tekeillä toinenkin ylemmän ammattikorkeakoulun päättötyö, jossa perehdytään syvällisemmin sisäiseen viestintään. Siinä otetaan tähänkin asiaan enemmän kantaa.

Saadut käyttäjätunnukset eivät aina toimi ja tätä joutuu selvittämään puhelimesta. Tämä on selkeä epäkohta, mutta on eri asia, voidaanko tähän tehdä teknistä korjausta. Omana havaintona todettakoon, että usein käyttäjät kirjoittavat saamansa salasanat väärin tai eivät osaa vaihtaa salasanaa, kun järjestelmä vaatii ensimmäisellä kirjautumiskerralla vaihtamaan

salasanan. Joskus tehdyt käyttäjätunnukset eivät toimi, ennen kuin ylläpito vaihtaa salasanan uusiksi. Hälyttävänä ongelmana mainittiin, ettei käyttäjätunnuksia ole aina tullut. Kuitenkaan ei osattu sanoa, oliko tunnuksset jääneet tekemättä vaiko postitetut tunnuksset jääneet seikkailemaan jonnekin välille. Tekemättä jääneet tunnuksset eivät ole tietoturvan kannalta vaarallisia, mutta välille jääneet tehdyt tunnuksset ovat. Tämäkin näkökulma puoltaisi sähköistä järjestelmää.

Vapaa sana.

Tässä annettiin esimiehille mahdollisuus vapaaseen palautteeseen. Uudistusten tekeminen koettiin viisaaksi. Samalla toivottiin, ettei yhtään uutta ohjelmaa tulisi lisää, ellei joku vanha poistuisi. Tämä on linjassa useiden eri salasanojen kanssa, joka koetaan ja joka on ongelma. Edelleen toivottiin sähköistä järjestelmää, joka toimisi, vaikka nimetty pääkäyttäjä olisikin lomalla.

4.2.2 Käyttäjätunnusten hallintaan liittyvät kysymykset

Kuvaile lyhyesti nykyinen virallinen prosessi tarvittavista toimista (tietojärjestelmän/käyttäjätunnusten osalta), kun käyttäjä poistuu organisaation palveluksesta.

Kysymys on osittain kompa, koska virallista prosessia tilanteesta ei ole (tai ei ole ainakaan päättötyöntekijän tiedossa). Tämä jo itsessään on suuri tietoturvariski ja epäkohta. Kysymyksellä pyrittiin siis selvittämään, mitä esimiehet mieltävät tehtävän, kun käyttäjä poistuu organisaatiosta. Koska virallista prosessia ei ole, myös vastaukset hajosivat hieman. Viidessä vastauksessa kerrottiin, että pitää tehdä ilmoitus. Ilmoituksen kohteeksi mainittiin ohjelman vastuuhenkilö, helpdeskin sähköposti, pääkäyttäjä ja ylläpito. Kaikki ovat oikeita vastauksia, mutta vain, kun nämä kaikki osapuolet ovat mainittuna samassa yhteydessä. Tämä kuvastaa käyttäjätunnusten hallinnassa esiintyvää ongelmaa ja hajanaisuutta.

Huolestuttavimpana vastauksena oli esimiehen toteamus, että hän on ymmärtänyt, että tarpeettomat tunnukset poistetaan. Omien havaintojen mukaan tässä on ongelmana informaatiokatkos. Tieto ei kulje esimiesten, ylläpidon ja ohjelmien nimettyjen pääkäyttäjien välillä, kun käyttäjä poistuu organisaatiosta. Ongelmia tässä aiheuttaa myös se, ettei mistään näe, mihin kaikkialle kyseisellä käyttäjällä on tunnukset.

Kuka tai ketkä ovat vastuussa käyttäjätunnusten ylläpidosta?

Kysymyksellä haluttiin saada tietää, miten esimiehet hahmottavat käyttäjätunnusten hallinnan. ”Oikea” vastaushan on yksiselitteisesti ”kaikki”. Tässä suurin osa vastauksista vastuutti esimiehet. Esimiehillä on organisaatiossa erittäin iso rooli käyttäjätunnusten hallinnassa, mutta vastuuta on myös ylläpidolla, ohjelmien pääkäyttäjillä ja käyttäjillä itsellään. Positiivisena huomiona yhdessä vastauksessa oli maininta, että ylläpito toimii esimiehiltä tulleen tiedon varassa. Vastaus kuvastaa hyvää ymmärrystä asiasta. Monessa vastauksessa oli maininta myös ylläpidosta ja pääkäyttäjistä. Vastausten perusteella voidaan sanoa, että esimiehet ymmärtävät hyvin käyttäjätunnusten hallintaan liittyvän vastuun.

Mistä tai keneltä käyttäjätunnusten hallintaan liittyvät asetukset (mm. salasanan vanheneminen, koneen lukitseminen jne) tulevat?

Kysymyksellä haluttiin testata esimiesten tietämystä salasanoihin liittyen. Taustalla on noin vuosi sitten tapahtunut liittyminen sähköiseen potilastiedon arkistoon, jonka vaatimissa koulutuksissa on käsitelty myös salasanoja ja niiden uusia vaatimuksia. Vastausten perusteella esimiehet olivat tästäkin asiasta hyvin perillä, sillä vastuullisiksi nimettiin useassa vastauksessa ylläpidon lisäksi kaupungin tietoturvapoliitikka ja lainsäädäntö.

Oletko törmännyt ongelmiin käyttäjätunnusten hallinnan kanssa? Minkälaisiin?

Tällä pyrittiin selvittämään, onko käyttäjätunnusten hallinnassa ongelmia. Kysymys on hallinnan kehittämisen kannalta kriittinen. Ongelmina mainittiin aikaisemminkin esille

noussut epäkohta, etteivät käyttäjätunnukset oikeasti ole esimiesten hallinnassa millään lailla. Tunnusten voimassaoloaika aiheutti myös ongelmia – eritoten sijaisten kanssa. Käyttäjätunnuksia ja salasanoja koettiin olevan liikaa muistettavaksi. Salasanojen unohtaminen, varsinkin salasanan vaihdon yhteydessä, koettiin ongelmaksi. Tietoturvan kannalta ongelmana oli se, että samoja tunnuksia käytetään useassa eri ohjelmassa. Omat havainnot tukevat näitä ongelmia. Käyttäjät ovat usein hyvin hukassa salasanojen ja järjestelmien kanssa. Usein käyttäjä pyytää uutta salasanaa väärään järjestelmään, joka aiheuttaa sekaannusta ja joudutaan vaihtamaan useampia salasanoja.

Pitäisikö käyttäjätunnusten hallintaa mielestäsi kehittää? Jos kyllä, niin miten?

Kysymyksellä haluttiin osallistuttaa esimiehiä kehitysohjelmaan ja kalastella uusia ideoita tunnusten hallintaan. Useammassa vastauksessa toivottiin käyttäjätunnusten hallintaa web-tallennukseen. Esimiehille toivottiin pääsyä hallinnoimaan käyttäjätunnuksia ja mahdollisuutta vaihtaa salasana tai muuttaa tunnusten voimassaoloaika. Unohtuneen salasanan vaihtoon toivottiin kehitettäväksi sähköistä järjestelmää. Kertakirjautumisen tapaista yhtä käyttäjätunnusta kaikkiin järjestelmiin toivottiin myös, vaikkakin ajatuksen uskottiin olevan mahdoton toteuttaa käytännössä. Ilahduttavaa oli huomata esimiesten halu osallistua tunnusten hallintaan. Tähän on olemassa yksinkertaisia teknisiä ratkaisuja, joten asia vaatii lisäkeskustelua esimiesten kanssa. Sähköinen käyttäjätunnusten hallintajärjestelmä ratkaisisi useita esiintyviä ongelmia.

Vapaa sana

Lopuksi haluttiin esimiehille antaa mahdollisuus tuoda esille aiheeseen liittyviä, mielenpäällä olevia asioita, joita ei osaa ajatella tai kysyä. Ehkä kysely oli jo aiheuttanut kisaväsymyksen, koska tähän tuli vain yksi vastaus. Siinä tuotiin esille salasanojen hurja määrä: ”...niitä on niin paljon että ne on pakko pitää piilossa kirjallisina tai aamulla kun tulee töihin ensimmäisenä joutuu anomään vanhojen tunnusten vaihtamista uusiin...joka aamu”. Tämä kyllä kiteyttää ongelman hyvin; salasanoja on (liian)paljon eri järjestelmiin.

4.3 IT-tiimin haastattelut

Haastattelu on yksi käytetyimmistä tiedonkeruumenetelmistä sekä kehittämis- että tutkimustyössä. Haastattelulla saadaan kerättyä nopeasti syvällistäkin tietoa kehittämisen kohteesta. Kehittämistyössä haastattelu kannattaa yhdistää muihin menetelmiin, koska yleensä menetelmät tukevat hyvin toisiaan. Haastatteluja ovat muun muassa strukturoitu eli standardoitu lomakehaastattelu, teemahaastattelu, syvähaastattelu ja ryhmähaastattelu. Haastattelu voi kestää kymmenistä minuuteista useisiin tunteihin. Haastattelu on haastattelijan alulle panemaa ja ohjaamaa, etukäteen suunniteltua vuorovaikutusta. (Ojasalo & Moilanen & Ritalahti 2009, 95 – 96.)

Useassa keskustelussa oman työnsä ohella Effican pääkäyttöä tekevien henkilöiden kanssa esiin nousi käyttäjien salasanojen unohtelu. Varsinkin lomien jälkeen salasanojen vaihto työllistää kovasti. Salasanoihin liittyen jokainen ylläpitoa tekevä henkilö totesi osan käyttäjistä sekoittavan eri järjestelmät keskenään ja pyytävän usein muuttamaan salasanaa väärään järjestelmään. Varsinkin Effic- ja verkkotunnukset sotkeentuvat monella. Ennen eReseptin käyttöönottoa Effic-tunnuksen salasana piti olla kuusimerkkiä pitkä ja verkkotunnuksen vähintään kahdeksan. Tästä käyttäjille lähetetty ohjeistus tuotti kipakkaa palautetta, kun osa käyttäjistä koki ohjeiden olevan ristiriidassa.

It-tiimin palavereissa esille nousi ongelma tunnistaa käyttäjä, joka pyytää salasanan vaihtoa. Ylläpidolla ei ollut käytettävissä luotettavaa tapaa todentaa käyttäjä, joka yleensä soittaa puhelimella ja pyytää salasanan vaihtoa. Monesti käyttäjät soittivat vieläpä siviili- tai salaisesta numerosta. It-tiimissä ongelmaksi koettiin myös käyttäjätunnusten anomislomakkeen vajaa täyttö, jonka perusteella käyttäjälle oli vaikea luoda tunnukset kerralla oikein.

4.3.1 Kyselytutkimus ylläpidolle

Viidelle käyttäjien verkkotunnusten ylläpidosta vastaaville lähetettiin pieni kyselytutkimus varmistamaan käytyjen keskustelujen johtopäätökset. Kysely tehtiin Webropolia hyväksi käyttäen. Vastausaikaa oli lyhyt 11.5.2015 – 13.5.2015. Silti jokainen töissä ollut henkilö vastasi kyselyyn. Yksi henkilö oli ajankohtana lomalla. Kyselytutkimuksen vastaukset tukivat osaltaan myös tehtyjä omia havaintoja. Samoja asioita nousi esille niin ylläpidolle kuin esimiehille tehdyssä kyselyssä.

Mihin ongelmiin/haasteisiin olet törmännyt käyttäjätunnusten anomisessa?

Kysymyksen asettelu jo sinällään olettaa, että ongelmia on ollut. Toisaalta olisi hyvin ihmeellistä, jos ylläpitoa tekevät henkilöt eivät olisi ikinä törmänneet minkäänlaisiin ongelmiin. Kysymyksellä haluttiin tuoda esille polttavimmat ongelmat anomisprosessissa. Vastaukset olivat yhdenmukaisia käytyjen keskustelujen kanssa. Käyttäjätunnuksia ei aina anota kirjallisesti tai anomuslomake tulee myöhässä. Prosessia ei siis noudateta. Esille nousi myös puutteet anomuslomakkeessa, jolloin lisätietoja piti erikseen kysellä. Koettiin etteivät kaikki esimiehet ole täysin sitoutuneita huolehtimaan uusien käyttäjien tunnuksista tai muutoksista käyttäjätunnuksiin.

Mihin ongelmiin/haasteisiin olet törmännyt käyttäjätunnusten hallinnassa?

Tämäkin kysymys olettaa, että ongelmia on täytynyt jossain vaiheessa olla. Kysymyksen tarkoitus on kaivaa esille käyttäjätunnusten hallinnassa olevia ongelmia. Esille nousi hyvä huomio, että käyttäjätunnusten hallinta-käytännöt ovat muuttuneet ja hallinnointia on kehitetty vasta jälkijunassa. Anomuslomakkeissa on ollut puutteita. Tämäkin aiheuttaa sekaannusta siinä, mihin oikeusryhmään tai sähköpostin jakelulistalle kyseinen käyttäjä laitetaan. Käyttävät sekoittavat verkkotunnukset eri ohjelmien tunnuksiin, kirjautuvat väärillä tunnuksilla ja saavat tunnukset lukkoon. Esille nousi myös se, ettei yhtenäistä käytäntöä tunnusten tilasta käyttäjän poissaolon aikana ole. Vastauksissa ylivoimaisesti eniten mainittiin

asia, että it-puolelle ei tule tietoa käyttäjän työsuhteen päättymisestä.

Miten kehittäisit tunnusten anomisprosessia?

Tällä kysymyksellä haluttiin kartoittaa ylläpitoa tekevien henkilöiden kehittämisideoita. Esimiehiltä toimitettiin aktiivista toimintaa tunnusten anomisen yhteydessä niin, että tunnukset anottaisiin etukäteen. Suurimmassa osassa vastauksissa kaivattiin sähköistä järjestelmää nykyisen paperisen tilalle. Uudesta sähköisestä järjestelmästä annettiin useita ehdotuksia, jotka ovat yhteneväiset kehitysehdotusten kanssa kappaleessa 5.1. Esille nousi kiinnostava ajatus käyttäjän tunnistamisesta sähköisellä allekirjoituksella.

Miten kehittäisit tunnusten hallintaa?

Tälläkin kysymyksellä etsittiin tunnusten hallintaa tekevien henkilöiden ideoita hallinnan kehittämiseksi. Edelleen sähköistä järjestelmää toivottiin, jossa jokaiselle sovellukselle olisi oma anomis- ja hallinnointisivu. Myös Web-tallennuksen hyödyntäminen nousi esille. Mietittäväksi ehdotettiin myös ajatusta käyttäjätunnusten hallinnoinnin siirtämisestä esimiehille. Tätä asiaahan myös esimiehet toivoivat omassa kyselyssään. Kuten esimiehet, myös ylläpidon ihmiset toivoivat kattavaa järjestelmää, josta näkisi kerralla kaikki käyttäjän olemassa olevat tunnukset.

Millainen mielestäsi on ylläpidon ja esimiesten välinen yhteistyö it-asioissa?

Kysymys on siksi olennainen, että asioita hoidetaan yhteistyössä. Jos vuoropuhelussa ylläpidon ja esimiesten välillä on ongelmia, sitä ei voi mikään tekninen ratkaisu korjata. Ylläpito sai esimiehille tehdyssä kyselytutkimuksessa hyvät arvosanat auttamisesta. Suurta dramatiikkaa ylläpidonkaan vastauksissa ei ollut. Useammassa vastauksessa todettiin asian vaihtelevan; osan kanssa asiat toimivat oikein hyvin, osan kanssa huonommin. Tuotiin esille ajatus, että osa esimiehistä kokee it-asioiden olevan välttämätön paha. Tähän viitataan myös esimiesten kyselytutkimuksen vastausmäärän analysoinnissa sekä omissa havainnoissa.

Ehdottomasti asia, jota tulisi organisaatiossa käsitellä. Vastauksissa koettiin myös, etteivät esimiehet välttämättä arvosta tarpeeksi it-asioiden tärkeyttä tai niiden vaatimaa kovaa tarkkuutta ja työtä. Todettiin ettei esimiehillä voi olla asennetta, ettei hän hallitse atk-asioista. Tällöin esimiehen pitäisi hankkia tarpeellinen osaaminen.

4.4 Omat havainnot

Havainnointi on tärkeä ja hyödyllinen tutkimuksellisen kehittämistyön menetelmä. Sen avulla on mahdollista saada tietoa siitä, miten ihmiset käyttäytyvät ja mitä luonnollisessa toimintaympäristössä tapahtuu. Tutkimuksellinen havainnointi ei ole satunnaista katselemista, vaan systemaattista tarkkailua. Aineistoa voidaan kerätä sekä luonnollisessa että keinotekoisissa tilanteissa. Havainnointia käytetään joko itsenäisesti tai haastattelun tai kyselyn lisänä ja tukena. Menetelmä mahdollistaa pääsyn tapahtumien luonnollisiin ympäristöihin. Sen avulla on mahdollista saada tietoa siitä, toimivatko ihmiset niin kuin sanovat toimivansa. Havainnointi sopii hyvin kehittämistehtäviin, joiden kohteena on yksilön toiminta ja vuorovaikutus toisten kanssa. Havainnoimalla selvitetään, mitä siinä tapahtuu, mitä kohde tekee tai miten sitä käytetään. Havainnointi kohdistuu ennalta määritettyyn kohteeseen. Tulokset pyritään rekisteröimään välittömästi muistiin käyttämällä lomakkeita, päiväkirjaa tai videoimalla, valokuvaamalla tai äänittämällä tilanteita. (Ojasalo & Moilanen & Ritalahti 2009, 103 – 104.)

Käyttäjät unohtavat salasanoja varsinkin lomien aikana. Kesälomalta paluut työllistävät ylläpitoa paljon. Käyttäjät ottavat ylläpitoon yhteyttä puhelimitse, kun unohtunut tai lukkiutunut tunnus pitäisi vaihtaa. Usein ylläpidolla ei ole keinoa todentaa soittava henkilö. Monesti käyttäjä soittaa tuntemattomasta- tai siviilinumeroista. Prosessin mukaan vaihdettu salasana pitäisi postittaa sisäisellä postilla käyttäjällä, mutta tämä on aivan liian hidas keino, kun käyttäjä on menossa esimerkiksi yövuoroon vuodeosastolle tai vanhainkotiin.

Käyttäjän poistuessa organisaation palveluksesta, tietoa ei muisteta ilmoittaa ylläpidolla ja käyttäjätunnukset jäävät roikkumaan. Käyttäjätunnusten lukitsemiselle tai poistamiselle ei ole olemassa tunnettua prosessia. Ylläpidolle ei ilmoiteta myöskään silloin, kun käyttäjä siirtyy työskentelemään eri toimipaikassa. Tämä olisi kriittinen tieto siksi, että aktiivihakemiston hakemistopuu pysyisi ajan tasalla. Siellä käyttäjät ovat sijoiteltu paikkakunnittain ja tehtävittäin/osastoittain. Ajantasaisuus helpottaa ylläpitoa ja muun muassa pääsynhallintaa.

Tunnusten anomisprosessi on liian hidas. Pahimmillaan se kestää kaksi viikkoa. Käyttäjät – varsinkin harjoittelijat - joutuvat kyselemään käyttäjätunnustensa perään tunnusten viipyessä. Tällaisissa tapauksissa käyttäjät antavat omat käyttäjätunnuksensa toisten käyttöön niin, että esimerkiksi harjoittelija voi tehdä tarvittavat kirjaukset potilastietojärjestelmään. Käyttäjätunnuslomakkeita postitetaan tietyille it-tiimin jäsenelle. Tämä aiheuttaa pitkiäkin viivästymisiä, kun kyseinen henkilö sattuu olemaan lomalla tai muuten pidempään poissa töistä. Nimettyjä kirjeitä ei voida aukoa ilman kyseisen henkilön suostumusta. Nykyistä tunnusten anomisprosessia hidastaa myös se, etteivät esimiehet tee anomuslomaketta työsopimuksen teon yhteydessä ja lähetä sitä it-tiimille. Tällöin it-tiimillä olisi aikaa tehdä uudelle työntekijälle tunnukset etukäteen valmiiksi.

Tunnusten anomislomake on osittain sekava, eikä ole täysin ajan tasalla. Esimiehillä on vaikeuksia hahmottaa, mitä kaikkea tietoa täytettävään lomakkeeseen tulisi laittaa. Tietotekninen sanasto on esimiehille tuntematonta. Käyttäjätunnuksia tehdessä ongelmia tuottaa myös käsin kirjoitetut anomuslomakkeet. Usein käsiala on epäselvää ja esimerkiksi käyttäjän nimestä ei tahdo saada selvää.

Tietoturvaan liittyen käyttäjille pitäisi järjestää lisäkoulutusta. Mikä onkaan helpompi tapa ”murtautua” tietojärjestelmään, kuin urkkia käyttäjätunnus ja salasana selville? Omien havaintojen perusteella tämä luultavasti onnistuisi pelkästään esittäytymällä ylläpitäjäksi tai muuksi ammattihenkilöksi ja kysymällä käyttäjältä tunnuksia. Laitetiloihin tai vastaaviin

pääsyä kysyessä ei henkilökorttia tai muuta tunnistetietoa yleensä kysytä eli ihmiset ovat liian luottavaisia.

Sähköpostitunnusten anomisesta tehtiin havainto, että prosessi on tavattoman hidas. Sähköpostitunnusten anomislomakkeen oli käyttäjä allekirjoittanut 29.7.2014. Esimies oli allekirjoittanut anomuksen 30.7.2014, jonka jälkeen anomus oli postitettu it-tuelle sisäisellä postilla. Anomus saapui it-suunnittelijalle 8.8.2014, jolloin sähköpostitunnukset luotiin, tulostettiin ja postitettiin käyttäjälle. Arvioitiin käyttäjän saavan tunnukset 12. tai 13.8. Tämä tarkoittaa sitä, että sähköpostitunnusten saanti kesti kaksi viikkoa. Alla olevasta prosessikaaviosta näkee, kuinka sisäinen posti käsittelee tunnusanomuksen kahdesti prosessin aikana.

Sähköpostitunnuksen anomislomakkeesta tehtiin havainto, että lomake ei vastaa täysin todellisuutta. Ylläpidon tunnusten luomista vaikeutti sähköpostin postituslistat. Lomakkeessa olevia postituslistoja ei löytynyt saman nimisinä sähköpostin hallinnasta. Ilman hiljaista tietoa ylläpidon oli useasti mahdotonta liittää käyttäjä anottuihin postituslistoihin. Havaintojen mukaan käytettävät ja tarvittavat postituslistat ovat epäselviä myös esimiehille.

5 KEHITYSSUUNNITELMA

Kyselytutkimusten, haastattelujen ja omien havaintojen pohjalta on perusteltua väittää, että käyttäjätunnusten anomien ja hallinta tarvitsevat sähköisen järjestelmän. Sähköisellä järjestelmällä on monia etuja. Se poistaa sisäisen postin aiheuttaman viiveen ja nopeuttaa prosessia huomattavasti. Oikein säädettyinä järjestelmä poistaa myös tunnusten anomisessa esiintyvän henkilöitymisen, joka voi aiheuttaa viivettä tai tunnuksia ei tule. Sähköinen järjestelmä parantaa dokumentoinnin tasoa, koska tunnuksista saadaan tehtyä tietovarasto ilman tulostusta paperille. Tämä parantaa tunnusten hallintaa varsinkin tilanteissa, joissa käyttäjä poistuu organisaation palveluksesta. Esimies, pääkäyttäjät ja ylläpito näkevät järjestelmästä, mihin kaikkiin järjestelmiin palveluksesta poistuvalla käyttäjällä on tunnuksia. Järjestelmä tarjoaa esimiehille mahdollisuuden hallinnoida tunnuksia ainakin jossain muodossa. Tätä peräänkuulutettiin tutkimuksen tuloksissa.

Käytössä olevia lomakkeita tulee päivittää ajantasalle. Lomakkeita pitää yrittää muokata helpommin ymmärrettäväksi. Kehitystyössä olisi hyvä olla mukana ylläpidon lisäksi esimiehiä. Muutaman esimiehen kanssa voisi käydä rauhassa koko tunnusten anomisprosessin ja hallinnan läpi. Tämä tuo lisätietoa, miten lomakkeita pitää muokata.

Sähköisen järjestelmän lisäksi on mahdollisuuksien mukaan hankittavia ohjelmistoja pyrittävä integroimaan suoraan aktiivihakemistoon. Tämä poistaa aina tarpeen yksiltä lisätunnuksilta ja salasanoilta. Mahdollisuus integroida ohjelmisto aktiivihakemistoon käyttäjän tunnistamiseksi on nostettava yhdeksi vaatimuskohdaksi ohjelmistoja kartoittaessa ja hankkiessa. Integrointi aktiivihakemistoon ei ole aina mahdollista, mutta sitä kannattaa ehdottomasti kysellä ohjelmistojen toimittajilta. Kannattaa ainakin tutkia kertakirjautumisen käyttömahdollisuutta osassa käytössä olevista ohjelmistoista.

Lukemattomien käyttäjätunnusten ja salasanojen viidakkoon on ajauduttu pitkän ajan kuluessa hiljalleen, kun tietojärjestelmiä on kehitetty ja hankittu lisää ohjelmistoja. Nyt on paikallaan kokonaiskuvan hahmottaminen ja varsinkin käyttäjätunnusten hallinnan miettiminen isommassa mittakaavassa uusiksi. Työ lähtee tietoturvapoliittikan päivittämisestä. Sen puitteissa luodaan ja päivitetään tarvittavat prosessit. Kehitystyöhön on suotavaa ottaa esimiehet mukaan. Kehitystyössä pitää huomioida myös ulkopuoliset sidosryhmät, kuten ulkoistettu helpdesk, ostopalveluna tuotettu lääkäripäivystys ja ohjelmistojen etätuki ja –ylläpito. Tunnusten anomisprosessi on sinällään kunnossa, mutta se pitää saada sähköiseksi.

5.1 Sähköinen järjestelmä

Sähköiset järjestelmät voisi jakaa kolmeen eri tasoon. Ensimmäisellä tasolla järjestelmä on lähinnä netissä täytettävä web-lomake, joka napin painalluksella toimittaa täytetyn lomakkeen tarvittaville henkilöille esimerkiksi sähköpostilla. Pääsyä järjestelmään voisi rajata käyttäjätunnuksilla, pitämällä palvelu organisaation sisäverkossa ja estämällä palveluun ulkoverkosta. Pienellä ohjelmointityöllä lomakkeesta voisi luoda sellaisen, jossa ennen lähetystä ohjelma tarkistaa, että kaikki tarvittavat kentät ja kohdat ovat täytetty. Ongelmana tässä on edelleenkin vähäinen tunnusten hallinnan puute sekä jälleen yksien käyttäjätunnusten lisäys.

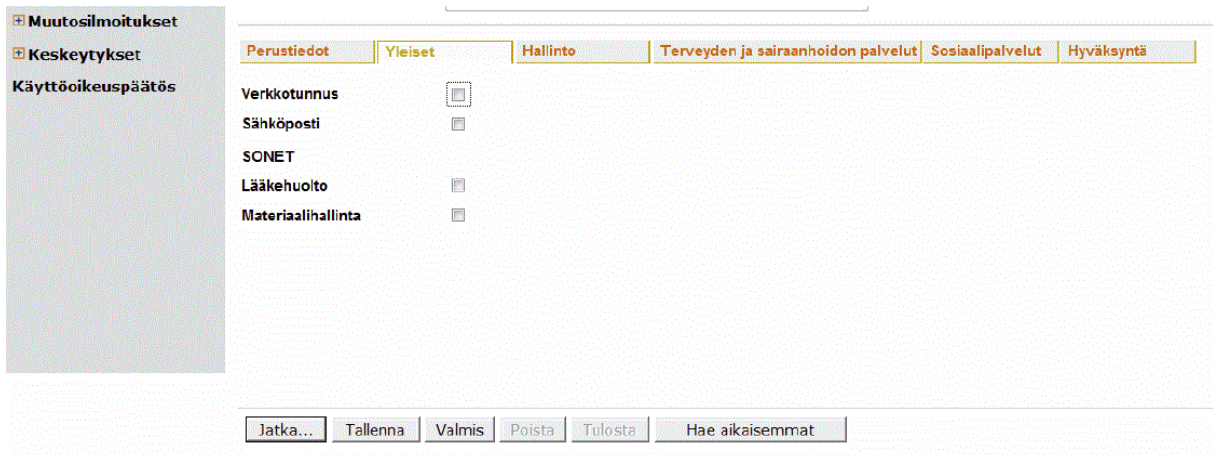
Hieman kehittyneemmässä järjestelmässä taustalla olisi tietokanta, johon kerätään käyttäjät ja heidän tunnuksensa eri järjestelmiin. Tietoturvasyistä ainakaan salasanoja ei tule tallentaa tietokantaan. Järjestelmä voi edelleen olla vain organisaation sisäverkossa. Nyt esimiehet voisivat tehdä järjestelmän kautta ylläpidolle muutospyyntöjä käyttäjätunnuksien oikeuksiin tai poistoihin. Etuna ensimmäiseen versioon parempi dokumentaatio ja monipuolisemmat käyttäjätunnuksen hallintatyökalut. Näiden kahden järjestelmän osalta etuna on myös hankintahinta. Kummassakin tapauksessa on mahdollista tuottaa järjestelmä omilla käytössä olevilla resursseilla. Ongelmana edelleen yhden lisäkäyttäjätunnukset sekä ylläpidon kannalta

ylimääräinen työmäärä eri järjestelmien välillä.

Kehittyneimmissä järjestelmissä sähköinen järjestelmä kommunikoi suoraan organisaation aktiivihakemiston kanssa. Esimiehet, pääkäyttäjät ja ylläpito kirjautuvat järjestelmään olemassa olevilla verkkotunnuksilla, jolloin lisää muistettavia salasanoja ei tule. Myös käyttäjät voivat tietyn reunaehdoin kirjautua järjestelmään ja vaihtaa unohtuneen salasanansa itse. Esimies voisi käytännössä tehdä tunnukset käyttäjälle itse. Järjestelmä voisi generoida käyttäjällä salasanan ja esimies luoda käyttäjätunnuksen ohjeistuksen mukaan. Etuna ylläpidon työmäärän väheneminen sekä esimiesten hallintamahdollisuus käyttäjätunnuksien osalta. Ongelma se, että tällaisia järjestelmiä ei käytännössä voi enää tehdä omana työnä, vaan on tilattava toimittajalta. Tämä vaatii siis eniten rahaa ja aikaa sekä suunnitteluun että itse ohjelmointityöhön tai valmiiden ohjelmistojen kartoittamiseen, vertailuun ja kilpailutukseen.

5.2 Web-tallennus

Sote-Helmella on käytössä CGI:n toimittama web-tallennus. Kyseisellä ohjelmalla anotaan ja hallitaan muun muassa kesälomia ja palkattomia vapaita. Käyttäjätunnuksia järjestelmään hallinnoivat palkanlaskijat, jotka toimivat myös ohjelmiston pääkäyttäjinä. Kyselytutkimuksessa ehdotettiin käyttäjätunnusten hallintaa lisättäväksi web-tallennukseen. Tämä on mahdollista. Ainakin yhdellä lähialueen kaupungilla on kyseinen järjestelmä käytössä. Web-tallennuksessa käyttäjän perustiedoissa otetaan kantaa myös käyttäjän pääsyoikeuksiin yleisiin tietojärjestelmiin (kuvio 6), hallinnon tietojärjestelmiin (kuvio 7), terveydenhuollon tietojärjestelmiin (kuvio 8) ja sosiaalihuollon tietojärjestelmiin (kuvio 9). Näin esimiehet voivat helposti anoa ja hallita työntekijöidensä tunnuksia eri järjestelmiin. Samalla dokumentaatio kunkin käyttäjän tunnuksista eri järjestelmiin pysyy ajan tasalla.



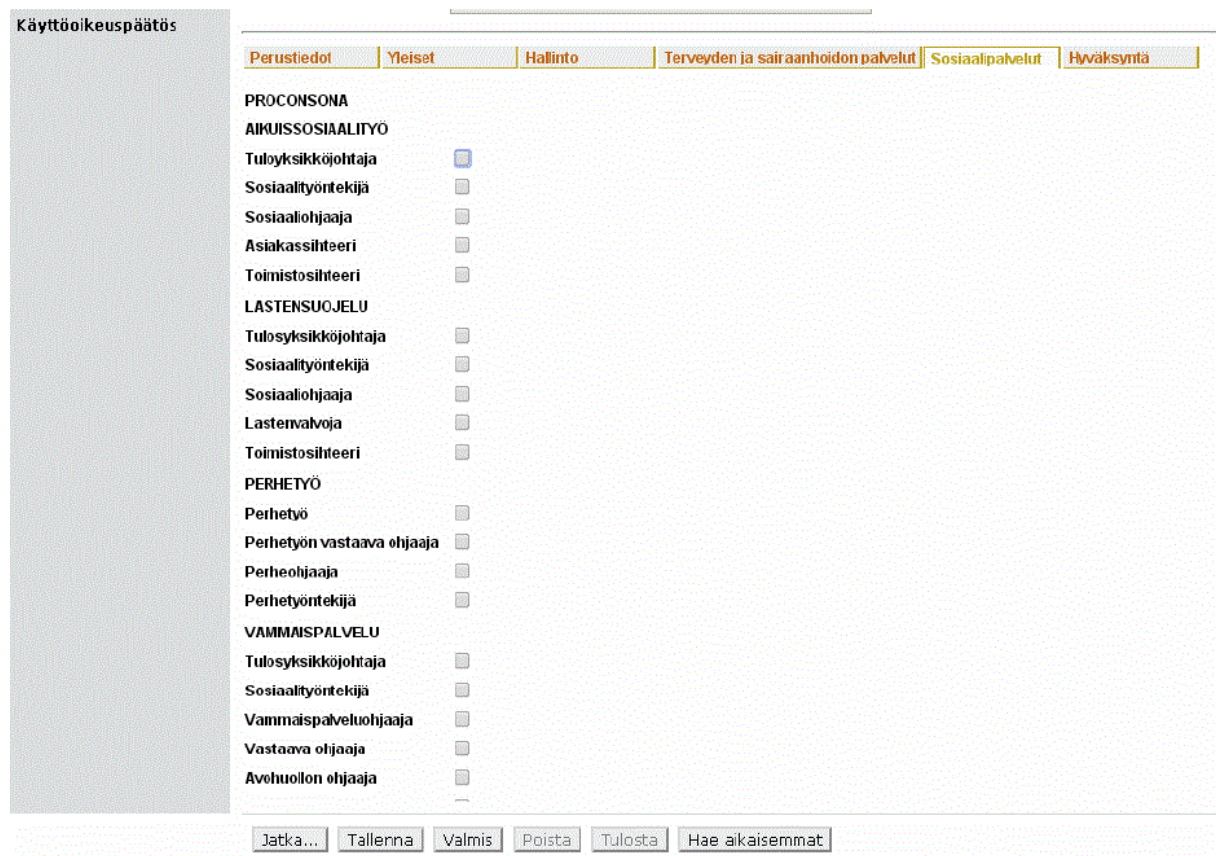
KUVIO 6. CGI:n Web-tallennus, käyttäjän perustiedot ja pääsy yleisiin ohjelmistoihin.



KUVIO 7. CGI:n Web-tallennus, käyttäjän pääsyoikeudet hallinnon ohjelmistoihin.



KUVIO 8. CGI:n Web-tallennus, käyttäjän pääsy terveydenhuollon ohjelmiin.



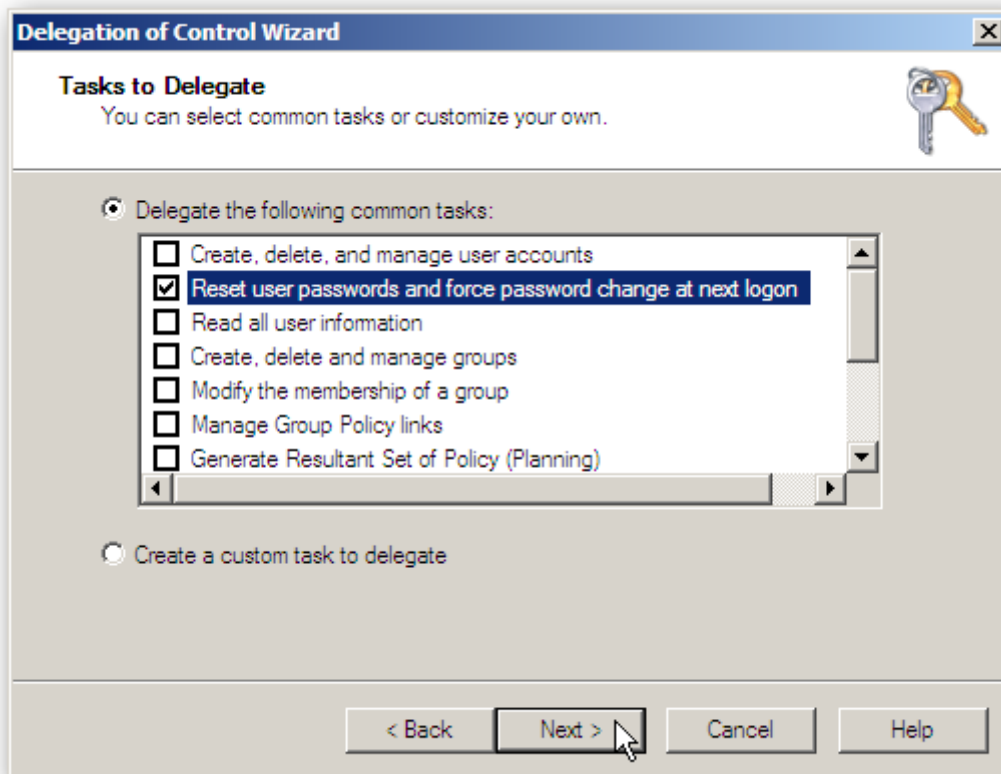
KUVIO 9. CGI:n Web-tallennus, käyttäjän oikeudet sosiaalihuollon ohjelmiin.

Tämä ratkaisu olisi laajennettavissa sosiaali- ja terveystieteiden lisäksi kaikkiin kaupungin toimintoihin, kuten hallintoon ja sivistyspuolelle. Esimiehille ei tulisi uusia käyttäjätunnuksia ja salasanoja muistettavaksi, koska käytettäisiin hyväksi jo olemassa olevaa järjestelmää. Pääkäyttäjänä toimivat palkanlaskijat eivät tarvitse lisäkoulutusta. Ohjelmasta saa tarvittaessa tulosten käyttäjän tunnuksista eri järjestelmiin. Esimies voi luotettavasti todentaa käyttäjän henkilökohtaisen tuntemisen, nimen ja sosiaaliturvatunnuksen avulla. Hankintakustannuksia tulisi jonkin verran ja nämä selviäisivät nopeasti kysyttäessä CGI:lta tarjous. Arvioin että paras ja kustannustehokkain ratkaisu käyttäjätunnusten hallintaan.

5.3 Aktiivihakemiston hallintaoikeuksien delegointi

On myös mahdollista antaa esimiehille rajoitetut oikeudet hallita aktiivihakemistoa tai aktiivihakemiston tiettyjä organisatorisia yksiköitä (kuviot 10). Tämä vastaa suoraan esimiehille tehdyssä kyselyssä ilmitulleisiin toiveisiin salasanoiden hallinnasta verkon osalta. Halukkaille esimiehille voisi delegoida oman toimipisteensä organisatorisen yksikön hallinnan käyttäjien osalta. Näin on tehtykin esimerkiksi sivistyspuolella ja oman työn ohella Effican pääkäyttöä tekeville. He saavat tehdä ja hallinnoida käyttäjätunnuksia suoraan aktiivihakemistosta omalla työasemallaan.

Käyttöönotto edellyttää Windows-käyttöjärjestelmän osien asentamista työasemalle, mutta ei lisäinvestointeja. Tällä voitaisiin poistaa kyselyssä esiin tulleita ongelmia salasanoiden nollauksessa sekä parantaa tietoturvaa liittyen salasanoiden uusimiseen ja käyttäjän todentamiseen. Työasemalle tehtävän paikallisen asennuksen lisäksi halukkaille esimiehille on suotavaa pitää asiasta käyttökoulutus sekä laatia mielellään kuvalliset rautalanka-ohjeet.



KUVIO 10. Microsoft Windows Server 2008, aktiivihakemiston ohjattu oikeuksien delegointi.

6 YHTEENVETO JA POHDINTA

Opinnäytetyön tavoitteena oli tutkia Sote-Helmen käyttäjätunnusten anomisprosessia ja käyttäjätunnusten hallintaa. Haluttiin kartoittaa prosesseissa mahdollisesti piilevät ongelmat. Tätä lähdettiin tutkimaan laadullisen tutkimuksen menetelmillä. Uusia käyttäjätunnuksia ja olemassa oleviin tunnuksiin muutoksia anoville esimiehille tehtiin kyselytutkimus. Käyttäjätunnuksia ylläpitäviä it-tiimin jäseniä haastateltiin epävirallisesti töiden ohessa. Tätä täydennettiin lyhyellä kyselytutkimuksella. Kolmantena menetelmänä käytettiin päättötyön tekijän omia havaintoja organisaatiossa.

Tutkimuksessa saatiin selkeitä tuloksia. Ongelmakohtina käyttäjätunnusten anomiseen liittyen esiin nousivat prosessin hitaus, kankeus ja epävarmuus. Prosessin noudattamatta jättäminen koettiin myös ongelmaksi. Anomislomakkeiden kanssa ongelmia aiheuttivat epäselvyys ja ajantasaisuus. Omat havainnot ja kyselytutkimus esimiehille osoittivat, että nykyinen tunnusten anomisprosessi on hidas eikä vastaa tätä päivää tai esimiesten tarpeita. Ylläpito koki, etteivät kaikki esimiehet noudata tunnusten anomisprosessia. Anomislomakkeet olivat usein täytetty puutteellisesti tai täytetty epäselvällä käsialalla.

Käyttäjätunnusten hallintaan liittyen ongelmiksi koettiin käyttäjien salasanojen unohtelu sekä liian monet salasanat ja käyttäjätunnukset. Ylläpidolle aiheutti ongelmia käyttäjien eri ohjelmien ja tunnusten sekoittaminen keskenään. Tukipyyntöjen yhteydessä käyttäjien todentamisessa oli ongelmia. Isona tietoturvaan liittyvänä ongelmana havaittiin, ettei käyttäjille tarkoitettu tietoturvataulu ollut kattavasti esillä. Ylläpito ei saanut tietoa organisaatiosta poistuvasta käyttäjästä. Muutoksen haku käyttäjätunnuksiin koettiin esimiesten keskuudessa vaikeaksi. Ongelmaksi koettiin myös se, ettei käyttäjälle myönnettyjä tunnuksia ole dokumentoituina mihinkään, eikä esimies tai ylläpito pääse niitä mitenkään tutkimaan. Tämä hankaloittaa hallintaa. Käyttäjätunnusten voimassaoloajan hallinta koettiin myös ongelmalliseksi – varsinkin vuorotyötä tai sijaisuuksia tekevien henkilöiden osalta.

Sekä esimiesten että ylläpidon mielestä organisaatio tarvitsee sähköisen järjestelmän nykyisen paperilomakkeen tilalle. Ylläpidosta toivottiin esimiehille isompaa roolia käyttäjätunnusten hallinnassa ja esimiehet toivoivat isompaa mahdollisuutta hallita työntekijöidensä käyttäjätunnuksia.

Esimiehet kannattaa ottaa aktiivisesti mukaan käyttäjätunnusten hallintaan. Heille asennetaan työasemille ohjelma käyttäjätunnusten hallintaan ja annetaan oikeudet hallita oman yksikkönsä tunnuksia. Tästä kannattaa järjestää koulutusta. Tämä helpottaa ylläpidon työkuormaa ja parantaa esimiesten mahdollisuutta hallita tunnuksia. Eri ohjelmien käyttäjätunnusten hallintaan pitää hankkia tai kehittää sähköinen järjestelmä. Kannattaa tutustua markkinoilla oleviin valmiisiin ohjelmistoihin, mutta taloudellisesti järkevintä on hyödyntää olemassa olevaa CGI:n Web-tallennus ohjelmistoa. Naapurikunnassa on olemassa tähän valmis malli tuotantokäytössä.

Jatkokehittämisessä kannattaa aloittaa tietoturvakartoituksesta ja tietoturvan kattavammasta käsittelystä. Tässä työssä on nostettu esille ongelmia tietoturvassa ja terveystoimen erityispiirteitä, jotka korostavat tietoturvan tärkeyttä. Jatkokehittämiselle on aihetta myös korttikirjautumisen käyttöönoton tutkimisessa. Tämä laajentaisi sähköisessä potilastiedon arkistossa ja sähköisessä lääkemääräyksessä käytössä olevien varmennekorttien käyttöä. Kyselytutkimusten valossa jatkokehittämistä vaativat myös organisaation sisäinen viestintä ja käyttäjätunnusten hallintaprosessi. Käyttäjätunnusten hallintaan ei ole tällä hetkellä olemassa virallista prosessia.

Tutkimusongelma laajentui ja rajautui tarkemmin aloitusseminaarin jälkeen paljon. Pidetyt seminaarit ohjasivat työtä hyvin eteenpäin antaen hyviä neuvoja ja näkökulmia. Omien havaintojen kirjaaminen ylös auttoi pitämään päättöyön mielessä ja kehittymässä päivätyön ohessa. Päättöyön tekijän työskentely toimeksiantajan palveluksessa oli hieman kaksiteräinen

miekka. Toisaalta kyselyn ja havaintojen tekeminen oli helppoa ja aihe tuttu, mutta toisaalta tuttu tutkimusympäristö aiheutti putkinäköisyyttä. Koulun ruokalassa käydyt keskustelut päättötyöstä luokkatovereiden kanssa auttoivat omalta osaltaan työn edistymistä. Aina työn edistyttyä osan matkaa, viimeisin versio lähetettiin päättötyön ohjaajalle. Hän antoi palautetta ja osoitti työssä kehityskohteita ja puutteita. Tämä auttoi muokkaamaan työstä loogisesti etenevän kokonaisuuden ja oli hyvä toimintatapa lopputuloksen kannalta.

Käytetyt tutkimusmenetelmät sopivat tutkimusongelmaan hyvin. Tulosten pohjalta saadaan konkreettisia kehittämistoimenpiteitä. Työ antaa hyvin eväitä ylläpidolle kehittää toimintaa. Päättötyön tekijä tuli uutena työntekijänä toimeksiantajan organisaatioon 2012. Kahden ja puolen vuoden aikana tehtyjen omien havaintojen painoarvo on suuri, koska niitä on voitu tehdä varsinkin työsuhteen alussa ”ulkopuolisen” silmin. Esimiehille tehty kyselytutkimus toi ”vastapuolen” näkökannan ja kokemat ongelmat esille. Tutkimusten teko oli helppoa, koska päättötyön tekijä tunsikin henkilökohtaisesti suurimman osan esimiehistä. Kyselyyn vastanneiden esimiesten määrä oli pettymys. Esimiesten henkilökohtainen tunteminen asetti odotukset paljon korkeammalle. Webropol-kyselytyökalun käyttö oli helppoa.

Työn aikataulu venyi aika paljon suunnitellusta. Tähän vaikuttivat työkiireet ja raskas syyslukukausi 2014. Pienet suvantovaiheet työn tekemisessä auttoivat jäsentelemään työn rakennetta. Lähdemateriaalia käyttäjätunnusten hallintaan liittyen oli hankala löytää. Terveysalan lainsäädännöstä ja asetuksista löytyi tietoa todella hyvin. Suurin oppiminen tapahtui tällä osa-alueella.

LÄHDELUETTELO

Haapaveden kaupunki. Viitattu 13.7.2014, <http://www.haapavesi.fi/haapaveden-kaupunki/haapavesi-info.html>.

Järvinen, P. 2012. Arjen tietoturva: vinkit & ratkaisut. Jyväskylä: Docendo.

KanTa, Kansalliset auditointivaatimukset. Viitattu 13.7.2014, <http://www.kanta.fi/documents/12105/3983179/Kansalliset+auditointivaatimukset+terveydenhuollon+organisaatioille+v2+0.pdf/8be958a4-5968-4b02-b74e-d3c2075aec14>

KanTa, Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä. Viitattu 13.7.2014 <http://www.kanta.fi/fi/lainsaadanto>.

Kanta, Liittymisohje Kanta-palveluihin 2013. Viitattu 7.8.2014, http://www.kanta.fi/documents/12105/3494314/Liittymisohje+KanTa-palveluihin+v1+4_28062013_fi.pdf/b06967b7-d39f-429e-95d3-f984859ec9a6.

KanTa, Potilastiedon arkisto. Viitattu 13.7.2014, <http://www.kanta.fi/fi/web/ammattilaisille/earkiston-esittely>.

KanTa, Potilastiedon arkistoa käyttävät terveydenhuollon yksiköt. Viitattu 13.7.2014, <http://www.kanta.fi/fi/potilastiedon-arkistoa-kayttavat-terveydenhuollon-yksikot>.

Ojasalo, K & Moilanen, T & Ritalahti, J. 2009. Kehittämistyön menetelmät – Uudenlaista osaamista liiketoimintaan. Helsinki: WSOYpro Oy.

Redicom Oy. Kertakirjautuminen eSSO. Viitattu 24.10.2014, <http://www.kertakirjautuminen.fi/esso.php>.

Sosiaali- ja terveysministeriö, 2013. Lainsäädäntö. Viitattu 7.3.2015, http://www.stm.fi/sosiaali_ja_terveyspalvelut/tietohallinto/lainsaadanto

Sosiaali- ja terveysministeriö, 2012. Potilasasiakirjojen laatiminen ja käsittely. Opas

terveydenhuollolle. Viitattu 17.3.2015, http://www.stm.fi/c/document_library/get_file?folderId=5197397&name=DLFE-21316.pdf

Sosiaali- ja terveysministeriö, 2014. Potilasturvallisuus. Viitattu 4.4.2015, http://www.stm.fi/sosiaali_ja_terveyspalvelut/terveyspalvelut/potilasturvallisuus

Sosiaali- ja terveysministeriö, 2014. Terveyspalvelut. Viitattu 7.3.2014, http://www.stm.fi/sosiaali_ja_terveyspalvelut/terveyspalvelut

Sosiaali- ja terveystieteiden tutkimuskeskus Helmi. Viitattu 13.7.2014, <http://www.sotehelmi.fi/helmi/sote-helmi.html>.

TechRepublic A closer look at Windows Server 2008's Directory Users and Computers. Viitattu 7.8.2014, <http://www.techrepublic.com/blog/the-enterprise-cloud/a-closer-look-at-windows-server-2008s-active-directory-users-and-computers/>.

Terveyden ja hyvinvoinnin laitos, 2014. Potilasturvallisuus. Viitattu 4.4.2015, <https://www.thl.fi/fi/web/laatu-ja-potilasturvallisuus/potilasturvallisuus/mita-on-potilasturvallisuus>.

Valvira, 2015. Potilasasiakirjat. Viitattu 4.4.2015, http://www.valvira.fi/ohjaus_ja_valvonta/terveydenhuolto/potilasasiakirjat.

Valvira, 2015. Terveydenhuollon ammattihenkilöiden keskusrekisteri. Viitattu 28.3.2015, http://www.valvira.fi/tietopankki/rekisterit/terveydenhuollon_ammattihenkilot/julkiterhikki

LIITTEET

LIITE 1	Verkkotunnusten hakulomake
LIITE 2	Salassapitosopimus
LIITE 3	Effica-tunnusten hakulomake
LIITE 4	Verkkotunnusten myöntämislomake
LIITE 5	Kuvio käyttäjätunnusviidakosta
LIITE 6	Esimiesten kyselytutkimuksen kysymykset
LIITE 7	Ylläpidon kyselytutkimuksen kysymykset

Verkkotunnuslomake

Käyttöoikeuden hakijan tiedot:

Nimi: _____
Osasto: _____
Tehtävä / Toimipaikka: _____

Käyttöoikeudet ja käyttöoikeuksien muutokset tiedostopalveluihin (esimies täyttää)

L-levy: hallintokunta: _____
pääsy kansioihin L-levyllä: kaikkiin
 vain näihin _____
Muut verkkolevyt: näkyvänä _____ ja käyttötarkoitus _____
näkyvänä _____ ja käyttötarkoitus _____
Sovellusohjelmat: Efficca Digia tarkastaja LimsBOSS Spiro
 Karttaohjelma Rakennusvalvonta Titania
Muu: _____
Muut verkkokansiot: _____
Käyttöoikeusryhmät: _____

Käyttöoikeustunnuksen voimassaoloaika

Toistaiseksi Ajalle _____ / _____ 20____ - _____ / _____ 20____

Sitoudun käyttämään saamiani käyttöoikeuksia vastuullisesti ja olemaan luovuttamatta tunnusta ja salasanaa toiselle henkilölle.

____ / ____ 20____

Hakijan allekirjoitus

Hyväksyn yllämainitut käyttöoikeudet

____ / ____ 20____

Esimiehen allekirjoitus

Nimen selvennys

ATK-tuen merkintä:

Tunnus luotu ____ / ____ 20____

Allekirjoitus

SALASSAPITO- JA KÄYTTÄJÄSITOUMUS

Työasemien (sisältää tietoverkkoon langallisesti/langattomasti liitetyt atk-laitteet), tietoliikenneverkon ja atk-järjestelmien käyttöoikeudet annetaan vain niille, jotka ovat allekirjoittaneet tämän salassapito- ja käyttäjäsitoumuksen. Sitoumukset arkistoidaan sovitulla tavalla keskitetysti tuloyksiköittäin/vastuualueittain.

1. Salassapidosta tiedän (sote-toimi):

Salassapitovelvollisuudesta (asiakirjasalaisuus ja vaihtolovelvollisuus) säädetään useissa laeissa kuten mm.: Laki potilaan asemasta ja oikeuksista (785/1992, muut. 853/2000, 13 §), Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000, 14-19 §), Laki terveydenhuollon ammattihenkilöistä (550/1994, 17 §), Laki yksityisestä terveydenhuollosta (152/1990, 12 §), Työterveyshuoltolaki (743/1978, 6 §), Laki viranomaisten toiminnan julkisuudesta (621/1999, 22-23 §), Hallintolaki (434/2003, 13 §) ja Henkilötietolaki (523/1999, 33 §).

Potilastiedot ovat Potilaslain mukaan salassa pidettäviä. Palvelussuhteen tai muun työtehtävän aikana tai sen päätyttyä sivulliselle ei saa ilmaista työn vuoksi tietoon saatuja terveydenhuollon toimintayksikköä tai sen asiakkaita, sopimuskumppaneita tai muita yhteistyötahoja koskevia salassa pidettäviä tietoja. Potilaiden terveydentilatiетоjen lisäksi tällaisia ovat myös mm. liike- ja ammatillisaisuudet. Hoitosuhteessa *sivullisella* tarkoitetaan muita kuin asianomaisessa toimintayksikössä tai sen toimeksiannosta potilaan hoitoon tai siihen liittyviin tehtäviin osallistuvia henkilöitä (PotL 13 §).

Sosiaalihuollon asiakirjat, jotka sisältävät tietoja sosiaalihuollon asiakkaasta tai muusta yksityisestä henkilöstä, ovat salassa pidettäviä. Sosiaalihuollon järjestäjä tai tuottaja taikka niiden palveluksessa oleva ei saa paljastaa asiakirjan salassa pidettävää sisältöä tai tietoa, joka asiakirjaan merkittynä olisi salassa pidettävä, eikä muutakaan sosiaalihuollon tehtävissä toimissaan tietoonsa saamaansa seikkaa, josta on lailla säädetty vaihtolovelvollisuus (Sosiaalihuollon asiakaslaki 14-15 §).

Rekisterien katselu- tai käyttöoikeutta ei ole muihin kuin työtehtävien edellyttämiin tietoihin, esimerkiksi ei omiin eikä lähiomaisten potilastietoihin ilman hoitavan lääkärin lupaa. Ilman rekisteristä vastaavan kirjallista lupaa ei saa luovuttaa tai siirtää salassa pidettäviä asiakastietoja tai muuta salassa pidettävää tietoa, eikä tallentaa niitä toisiin rekistereihin, työaseman kiintolevylle, levykkeelle tai muille tallennuslaitteille.

2. Käyttäjätunnuksesta ja salasana tiedän:

Työasemaa saa käyttää vain omalla käyttäjätunnuksella ja salasanalla. Käyttäjätunnukset ovat henkilökohtaisia. Kukin vastaa käyttäjätunnuksellaan tehdyistä merkinnöistä.

Salasana on vaihdettava heti sen saamisen jälkeen ja myöhemmin tarvittaessa tai sovituin aikavälein.

Käyttäjätunnus ja salasana on pidettävä muistissa. Niitä ei saa antaa muiden tietoon.

Tietojärjestelmistä on kirjauduttava ulos tai työasema on lukittava välittömästi käytön jälkeen, ellei työasema ole käyttäjän valvonnassa.

3. Työaseman käytöstä tiedän:

Työasemassa saa käyttää vain kaupungin toimintayksikön hyväksymiä ja lisensoituja ohjelmia, jotka ovat ATK-yksikön asentamia ja tukemia tai erillisellä ATK-yksikön hyväksynnällä tavalla muun toimittajan asentamia ja tukemia.

Kaupungin hankkimia ohjelmia ei saa kopioida.

Työasemaa ei saa liittää verkkoon tai siirtää luvatta.

Samoja levykkeitä tai muita tietovälineitä ei saa käyttää työpaikalla ja sen ulkopuolella, jollei ole varmistautunut niiden viruksettomuudesta.

Epäiltäessä työaseman olevan tietokoneviruksen saastuttama, työasemalla työskentely on lopetettava välittömästi. Tietokoneviruksista on aina ilmoitettava ATK-yksikköön.

Työaseman käytössä on otettava huomioon tietoverkon ja palvelinlaitteiden rajoitettu kapasiteetti. Kuvia, grafiikkaa ja äänitiedostoja saa välittää verkossa tai tallentaa palvelimelle vain työtehtävien vaatiessa.

Työasemaa ei saa käyttää tiedostojen pysyvään säilytykseen.

Työasemaan talletettujen tiedostojen varmuuskopioimisesta vastaa kukin käyttäjä itse.

Palvelimilla olevien tiedostojen varmistuskopiointi hoidetaan keskitetysti tai järjestelmän pääkäyttäjän toimesta.

4. Sähköpostin ja Internet-yhteyksien käytöstä tiedän:

Sähköposti ja Internet-yhteydet on tarkoitettu pääsääntöisesti työtehtävien hoitoon.

Sähköpostin käytössä noudatetaan asiasta sovituja periaatteita.

Arkaluonteisia ja muita salassa pidettäviä tietoja ei saa lähettää ulkoisen sähköpostin välityksellä.

Virusriskin vuoksi ulkopuolelta tulevan sähköpostin liitetiedostoja ei saa avata, jos viesti tulee epäamääräisestä lähteestä. Viesti on syytä hävittää.

Sähköpostitietokirjeitä ja muuta roskapostia ei saa lähettää eikä välittää eteenpäin, vaan ne on tuhottava.

Internetistä ei saa kopioida ohjelmia.

5. Järjestelmäkohtaisista ohjeista tiedän:

Kukin käyttäjän on tutustuttava kaupungin yleisiin tietoturvaohjeisiin, ja mahdollisesti oman yksikkönsä ohjeisiin, sekä käyttämiensä tietojärjestelmien käyttöohjeisiin ja rekistereiden rekisteriselosteisiin.

Tietojärjestelmien käytöstä kertyy somenjälkkitietoa ja käyttöä seurataan.

6. Seuraamuksista tiedän:

Sääntöjen ja periaatteiden rikkomisesta käyttöoikeudet tietojärjestelmiin voidaan peruuttaa. Rikkomuksista tiedotetaan aina esimiehelle. Jos

kyseessä on toistuva tai vakava rikkomus, ryhdytään tapauksen edellyttämiin jatkotoimiin. Mikäli rikkomuksesta aiheutuu välittömästi tai välillisesti taloudellisia menetyksiä, voidaan päätyä vahingonkorvausvaatimuksiin (ks. tietosuojaikäkirja).

Tietojen väärinkäyttö tai tahallinen ohjeiden vastainen toiminta voi johtaa muun ohella rikosoikeudellisiin seuraamuksiin.

Olen lukenut/ymmärtänyt yllä olevan salassapito- ja käyttäjäsitoumuksen periaatteet ja sitoudun noudattamaan niitä.

Toimipaikka: _____ Pvm/..... 20....

Allekirjoitus ja nimen selvennys: _____

Esimiehen allekirjoitus ja nimen selvennys: _____

Haapaveden kaupunki/Sosiaali- ja terveystieteiden Helmi



EFFICA-KÄYTTÖOIKEUSLOMAKE

Tällä lomakkeella rekisteröidytään uudeksi käyttäjäksi Sosiaali- ja terv-piiri Helmen potilastietojärjestelmän käyttäjäksi. Tätä lomaketta käytetään myös jo olemassa olevan käyttäjätunnuksen oikeuksien muuttamiseen.

Käyttäjän nimi: Henkilötunnus: Terhikki-rekisteritunnus: Työyksikkö: Lähiosoite: Postinro ja-paikka

Erityishoitoa vaat. pot. hoitajat
 Farmaseutit
 Ravitsemusterapeutit
 Röntgenhoitajat
 Fysioterapeutti
 Koulukuraattori

Perheneuvola
 Puheterapeutit
 Päihdetyöntekijät
 Siikalatvan ambulanssin hoitajat
 Terveystieteiden ja hyvinvoinnin suunnittelija

Kehitysvammahuolto

- Haapaveden Helmikartanon katseluoikeudet
- Haapaveden Helmikartanon ohjaajat
- Haapaveden Kotirinteen ohjaajat
- Kestilän kehitysvammaisten asuntolan hoi
- Rantsilan toimintakeskuksen ohjaajat

Hammashoitola: (paikkakunta)

- hammashoitajat
- hammaslääkärit
- suuhygienistit

Lääkärit

- terveyskeskuslääkärit
- psykiatrit

Mielenterveysneuvola

- Mielenterveysneuvola
- Rantsilan tukikeskus

Neuvola: (paikkakunta)

- terveydenhoitaja
- terveyskeskusavustaja
- terveydenhuollon osastonhoitaja

Poliklinikka: (paikkakunta)

- sairaanhoitajat
- lähihoitaja/tka
- tekstinkäsittelijät
- ajanvaraus ja neuvonta

Laboratorio

- laboratoriohoitajat
- labran näytteenottajat

Vuodeosasto: (paikkakunta)

- sairaanhoitaja
- lähihoitaja/perush
- osastosihteerit
- fysioterapeutti

Kotihoito: (paikkakunta)

- kotisairaanhoitaja
- lähihoitaja/perushoit

Asumispalvelut: (paikkakunta)Palvelukeskus: (esim Pihlajisto)

- lähihoitaja/perush
- sairaanhoitaja
- osastonhoitaja
- sihteeri

EFFICA-KÄYTTÖOIKEUSLOMAKE

- Rantsilan ryhmäkodin hoitajat
- Rantsilan ryhmäkodin sairaanhoitajat

Muut Effica ohjelmat lisäksi _____
(esim Hallinta (asiaksiryhmät), Seuranta)

Käyttöoikeuksien hakijan ja hänen esimiehensä allekirjoitukset:

Hyväksyn hakijan edellä mainitut käyttöoikeudet hakijan työtehtäviin kuuluviksi. Ilmoitan pääkäyttäjälle viivyttämättä käyttöoikeuksiin vaikuttavista muutoksista

Otan vastaan edellä luetellut atk-käyttöoikeudet ja sitoudun noudattamaan terveyskeskuksen voimassa olevia tietoturvaohjeita. Olen yksin vastuussa tunnuksellani tehdyistä töistä.

_____	_____	_____	_____
Päiväys	Esimiehen allekirjoitus	Päiväys	Käyttäjän allekirjoitus

Käyttäjä tunnus voimassa asti: _____ (esimies ottaa Kantaa tähän!)

Atk-tukihenkilö täyttää:

Käyttäjätunnus: _____

Pvm: _____

VERKKOTUNNUKSET

Toimialue: SIIKATEPA

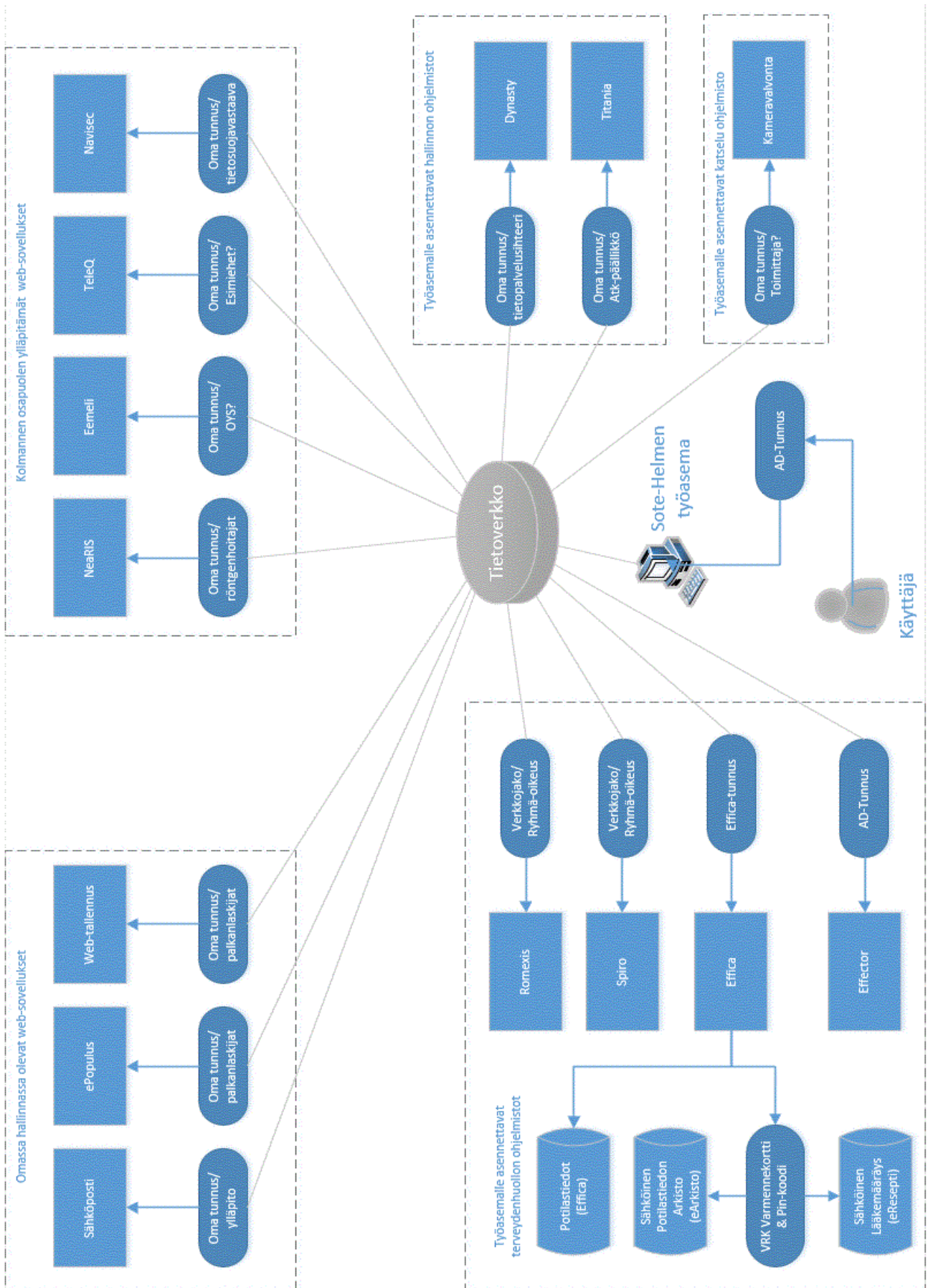
Käyttäjä:

Käyttäjän login-tunnus:

Salasana:

(salasana on muutettava 1.kirjautumisella)

Kotihakemisto:



1. Arvioi nykyistä tunnusten anomisprosessia väittämien mukaan arvosanoin 1-5 (1 huono, 2 välttävä, 3 tyydyttävä, 4, hyvä, 5 kiitettävä).

Ohjeistus tunnusten anomiseen on helposti löydettävissä.
Ohjeet tunnusten anomiseen ovat selkeät.
Nykyinen tunnusten anomisprosessi toimii sujuvasti.
Anomisprosessi on joustava.
Saan tarvittavat käyttäjätunnukset nopeasti.
Saan kerralla käyttäjätunnuksiin liittyvät asiat kuntoon.
Käyttäjätunnusten anomislomake on helppo täyttää.
Tarvittaessa saan apua ylläpidolta nopeasti.
Ylläpito tukee tarpeeksi.
Täytän käyttäjätunnusten anomislomakkeen valmiiksi työsopimuksen teon yhteydessä.
Nykyinen paperinen tunnusten anomisprosessi on riittävä.

2. Kuvaile lyhyesti nykyinen virallinen käyttäjätunnusten anomisprosessi.
3. Miten nykyinen käyttäjätunnusten anomisprosessi mielestäsi toimii?
4. Mitkä ovat nykyisen prosessin hyvät/huonot puolet?
5. Pitäisikö nykyistä prosessia mielestäsi kehittää? Jos kyllä, niin miten?
6. Vastaako nykyinen prosessi teidän tarpeita vai puuttuuko siitä kenties jotain?
7. Onko sinulla ollut ongelmia käyttäjätunnusten anomiseen liittyen? Jos on, niin minkälaisia?
8. Vapaa sana käyttäjätunnusten anomiseen liittyen

9. Arvioi seuraavassa nykyistä käyttäjätunnusten hallintaa (salasanojen vaihto/aukaisu/poisto/oikeuksien lisääminen) väittämien mukaan arvosanoin 1-5 (1 huono, 2 välttävä, 3 tyydyttävä, 4 hyvä, 5 kiitettävä).

Unohtuneen salasanan vaihtaminen on helppoa.
Lukitun käyttäjätunnuksen aukaisu on helppoa.
Käyttäjät unohtavat salasansa harvoin.
Salasanoja ei ole liikaa eri järjestelmiin.
Ohjeistus käyttäjätunnusten hallintaan on riittävä.
Käyttäjätunnuksiin liittyvä ohjeistus on helposti saatavilla.
Kaupungin tietoturvapoliittika on ajantasalla.
Käyttäjille tarkoitettu tietoturvataulu on näkyvillä.
Saan tarvittaessa apua ylläpidolta.
Saan tarvittaessa apua ylläpidolta nopeasti.
Käyttäjän poistuessa organisaation palveluksesta kaikki hänen käyttäjätunnuksensa tulee poistettua.
Ilmoitan käyttäjän poistumisesta organisaation palveluksesta ylläpidolle.
Muutoksenhaku käyttäjätunnuksiin on helppoa.
Muutoksen haku käyttäjätunnuksiin on ohjeistettu hyvin.
Käyttäjät ymmärtävät, mitä riskejä käyttäjätunnuksen ja salasanan joutumisesta vieraisiin käsiin liittyy.
Käyttäjät ovat sitoutuneita noudattamaan tietoturvapoliittikkaa.
Käyttäjät muistavat lukita tietokoneen poistuessaan työasemalta.
Käyttäjätunnuksia ja salasanoja ei ole kirjoitettu (muisti)lapuille työasemaan viereen näkyville (tai näppäimistön alle).

10. Kuvaile lyhyesti nykyinen virallinen prosessi tarvittavista toimista (tietojärjestelmän/käyttäjätunnusten osalta), kun käyttäjä poistuu organisaation palveluksesta.
11. Kuka tai ketkä ovat vastuussa käyttäjätunnusten ylläpidosta?
12. Mistä tai keneltä käyttäjätunnusten hallintaan liittyvät asetukset (mm. salasanan vanheneminen, koneen lukitseminen jne) tulevat?
13. Oletko törmännyt ongelmiin käyttäjätunnusten hallinnan kanssa? Minkälaisiin?
14. Pitäisikö käyttäjätunnusten hallintaa mielestäsi kehittää? Jos kyllä, niin miten?
15. Vapaasana käyttäjätunnusten hallintaan liittyen.

1. Mihin ongelmiin/haasteisiin olet törmännyt käyttäjätunnusten anomisessa?
2. Mihin ongelmiin/haasteisiin olet törmännyt käyttäjätunnusten hallinnassa?
3. Miten kehittäisit tunnusten anomisprosessia?
4. Miten kehittäisit tunnusten hallintaa?
5. Millainen mielestäsi on ylläpidon ja esimiesten välinen yhteistyö it-asioissa?