Ilmari Salo

KIRKKO-verkon uudistusprojekti

Metropolia Ammattikorkeakoulu

Tutkinto Insinööri

Tutkinto-ohjelma Tieto- ja viestintä

Opinnäytetyö

Päivämäärä 5.5.2021

Tiivistelmä

Tekijä(t):	Ilmari Salo
Otsikko:	KIRKKO-verkon uudistusprojekti
Sivumäärä:	37 sivua + 1 liitettä
Aika:	5.5.2021
Tutkinto:	Insinööri
Tutkinto-ohjelma:	Tieto- ja viestintä tekniikka
Suuntautumisvaihtoehto:	Verkko- ja pilvipalvelut
Ohjaaja(t):	Tapio Wikström Lehtori

Tämän työn tavoitteena on tarkastella Suomen evankelisluterilaisen kirkon nykyistä verkkoratkaisua ja tehdä ehdotus KIRKKO-verkon uudistamista varten. Työssä käydään läpi KIRKKO-verkon nykyinen tila ja tulevaisuuden visiot. KIRKKO-verkon kartoittaminen on tehty haastattelemalla kirkon IT-alueiden tietohallintopäälliköitä. Kartoituksessa tarkoituksena on etsiä tavat toteuttaa verkkoliitännät ja niiden määrä sekä KIRKKO-verkkoon liitettyjen liittymien nopeuksia ja verkkolaitteistoa. Työ sisältää myös muita uudistuksien kannalta oleellisia osa-alueita, kuten aihealuetta koskevaa lainsäädäntöä ja kirkon hallinnollista rakennetta.

Työssä lisäksi tarkastellaan muita kirkon IT-infrastruktuuriin tehtäviä uudistuksia, kuten pilvipalveluita. Uudistusehdotuksien tarkoituksena on luoda kirkon käyttöön käytännöllinen IT-infrastruktuuri, jota tulevaisuudessa voisi tarvittaessa muokata helpommin sen hetkisiä tarpeita vastaaviksi. Työn muut osa-alueet keskittyvät mahdollisiin muihin uudistuksiin, jotka voitaisiin käynnistää KIRKKO-verkon uudistuksen yhteydessä.

Ongelmien huomioon ottaminen on merkittävä osa työtä, koska uudistusprojekti on riippuvainen monesta eri toimielimestä ja lainsäädäntöön liittyvistä näkökohdista, jotka on otettava uudistuksen toteutuksessa huomioon.

Työn keskeinen ehdotus on hyödyntää liittymissä jatkossa langattomia ratkaisuja (4G). Jo nyt on syytä valmistua tulevaisuuden 5G-ratkaisuihin. Hallinnollisesti on syytä kehittää järjestelmää siten, että hallintaprosessista tulisi nykyistä helpompi. Tämä edellyttää sitä, että yksi taho tekee kirkon IT-ratkaisuja koskevat keskeiset päätökset. Laitehallintaa varten IT-ratkaisujen tulee olla kirkossa riittävän yhtenäisiä.

Koska työ on tehty tilaustyönä, se sisältää salassa pidettävää materiaalia. Viittaus niihin löytyy ei-julkisista liitetiedoista.

Abstract

Author(s):	Ilmari Salo
Title:	Upgrading the KIRKKO-verkko
Number of Pages:	37 pages + 1 appendices
Date:	5 May 2021
Degree:	Engineer
Degree Programme:	Information and Communication Technology
Specialisation option:	IOT and Cloud Computing
Instructor(s):	Tapio Wikström, Lector

The objective of this thesis is to take a closer look at the network infrastructure within the Evangelic-Lutheran church of Finland and make a proposal how to upgrade the KIRKKO-verkko (organization network of the Finnish church) network. This thesis was commissioned by the church coucil (kirkkohallitus) and includes classified sources.

This thesis includes the current situation of the KIRKKO-verkko and what the network should be like in the future. Mapping of the network has been done by interviewing areal IT-administration chiefs within the church. The purpose of the mapping is to find different types of network connections to the KIRKKO-verkko as well as the speed of these connection types. This also includes the amounts of the connections and what kind of network hardware is used inside the network. Another goal was to determine what kind of network hardware should be used.

There are other areas of the IT-infrastructure that could be upgraded as well, for example cloud-computing. Part of this thesis focuses on these other potential upgrades that could be made so that in the future the IT-infrastructure runs smoothly and has the possibility for further changes.

One part of the work is to take possible issues into account. In order to upgrade the KIRKKO-verkko there are a lot of different branches within the church and laws that must be noted in the project.

The main proposal of this thesis is to upgrade all the connection inside KIRKKO-verkko to use wireless 4G connections. In the future the goal is to prepare for the upgrade of the network to 5G connections. The proposal also includes ideas on how to make the administration inside the church easier so that only one decision making body could make choices regarding the IT-sector.

Sisällys

Sanasto

AD = Active Directory (käyttäjätietokanta ja hakemistopalvelu).
IT = Information technology. (Informaatiotekniikka tai tietotekniikka).
DHCP = Dynamic Host Configuration Protocol. (verkkoprotokolla, joka jakaa IP-osoitteita uusille verkkoon kytkeytyville laitteille).
O365 = Microsoft Office 365.
SCCM = System Center Configuration Manager. (Ohjelma, jonka avulla pystytään hallitsemaan suuria laitemääriä organisaatioissa).
DVV= Digi- ja väestötietovirasto.
EULA = End User License Agreement. (Loppukäyttäjän lisenssisopimus)
MAM = Mobile Application Management. (puhelimen ohjelmien hallinta).
MDM = Mobile Device Management. (puhelimen laitehallinta).
KS = Kirkon säädöskokoelma.
MFA = Multifactor authentication (monivaiheinen tunnistautuminen).
z-tunnus = Kirkon antama käyttäjätunnus kirkontyöntekijöille.
MPLS = Multiprotocol Label Switching. (Verkkojen reititys tekniikka).
VPN = Virtual Private Network. (Dataliikenteen salaava verkko-yhteys).
SD-Wan = Software Defined Wide Area Network. (Ohjelma, joka helpottaa verkon hallintaa).
MEM = Microsoft Endpoint Manager. (Ohjelma, joka on tarkoitettu laitehallintaan yrityksissä ja organisaatioissa).
DLP = Data loss prevention tai Data loss prevention. (Ohjelma, joka seuraa, havaitsee ja estää datan päätymisen ulkopuolisille).
Wlan = Wireless Local Area Network. (Langaton lähiverkko).
PEAP = Protected Extensible Authentiction Protocol. (Tunnistautumiseen liittyvä protokolla etenkin langattomissa verkoissa ja suorissa verkkoyhteyksissä).
M365 = Microsoft 365.
SSID = Service Set Identifier. (Langattoman lähiverkon verkkotunnus).
GDPR = General Data Protection Regulation. (Yleinen tietosuoja-asetus).

1 Johdanto

Opinnäytetyön tavoitteena on tehdä uudistusehdotus Suomen evankelisluterilaiselle kirkolle koskien verkkoarkkitehtuuria ja samalla pohtia, miten kirkon IT:n infrastruktuuria voisi modernisoida. Osa-alueina ovat kirkon oma organisaatioverkko (KIRKKO-verkko), pilvipalvelut, IT-tuki, laitehallinta ja tietoturva. Työssä käsitellään kirkon toimintaa koskettavaa julkisuuslainsäädäntöä ja tietoturvaa koskevaa lainsäädäntöä. Työssä tarkastellaan verkkoinfrastruktuuriin liittyviä vaihtoehtoja ja sitä, miten suurissa organisaatioissa verkkoa voidaan kehittää. Työ sisältää myös KIRKKO-verkon nykytilan ja pohdintoja tulevaisuuden visioista.

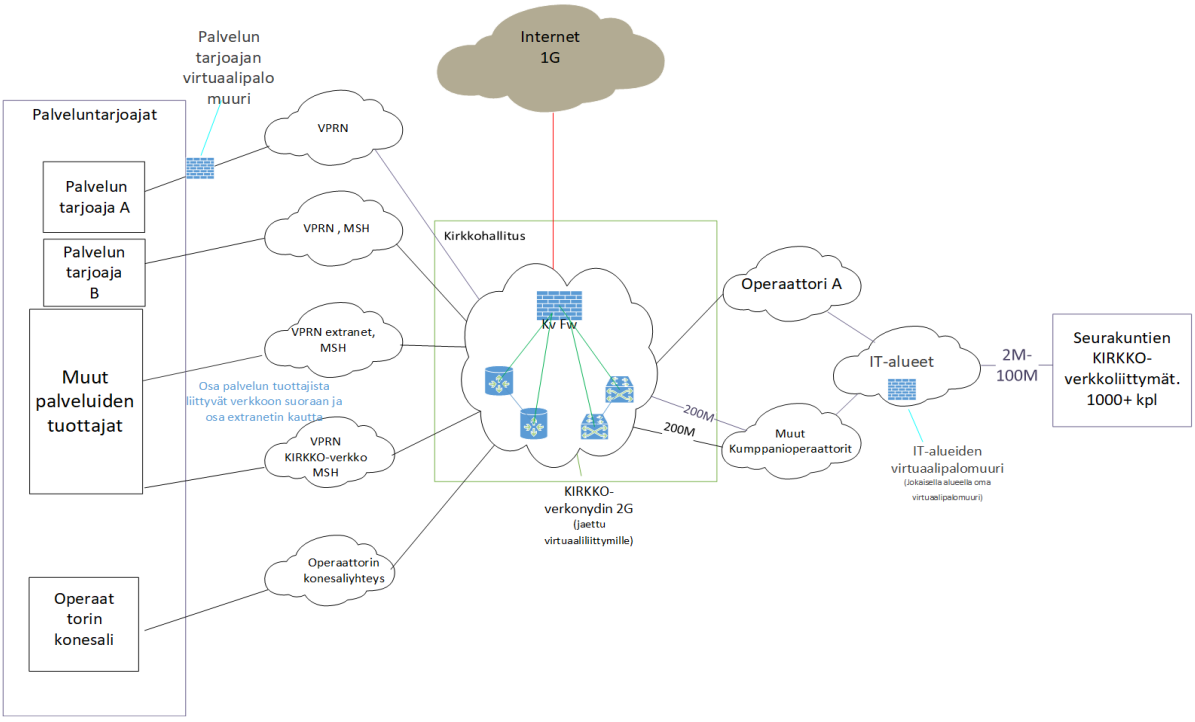
KIRKKO-verkon uudistusprojekti on suurimmaksi osaksi selvitystyö, jonka kirkkohallitus on opinnäytetyönä tilannut. Selvitystyötä varten on haastateltu kirkon omia IT-asiantuntijoita ympäri Suomea. KIRKKO-verkon uudistusprojektin päätarkoitus on luoda pohja tulevaisuuden IT-ratkaisuille. Kirkon hallinnollinen rakenne on uniikki muihin vastaaviin isoihin organisaatioihin verrattuna. Raportissa pyritään ottamaan huomioon kaikkien kirkon sisällä olevien IT-toimijoiden toiveet ja huolenaiheet koskien uudistusta.

2 KIRKKO-verkko ja sen kartoitus

KIRKKO-verkko on Suomen Evankelis-luterilaisen kirkon käyttöön rakennettu tietoliikenneinfrastruktuuri, joka perustuu kirkolle tehtyihin ratkaisuihin ja julkisiin tietoliikenneverkkoihin [1]. KIRKKO-verkossa toimii useampi operaattori. KIRKKO-verkko on rakennettu 90-luvun aikana sen ajan tarpeita vastaavaksi. Nykyään KIRKKO-verkkoa vaativat tarpeet pystytään toteuttamaan eri tavoin ilman erillistä verkkoa pohjana. Suurin syy KIRKKO-verkon olemassaoloon vielä nykypäivänä on kirkon viranomaistehtävät. Kirkon jäsentietojärjestelmä Kirjuri sisältää salassa pidettävää tietoa. Vielä toistaiseksi Kirjuri vaatii KIRKKO-verkkoyhteyden. Kirjuri sisältää arkaluontoisia henkilötietoja, joten tietoturvavaatimukset ovat merkittävät.

Seurakuntaliittymiä KIRKKO-verkkoon on kokonaisuudessaan yli 1000 ja palveluliittymiä 20–30 kappaletta. Jokainen seurakuntatalous saa tehdä omat sopimuksensa eri toimittajien kanssa. Kyseiset sopimukset pitää ottaa huomioon uudistuksessa. Jotkut seurakuntataloudet ovat ulkoistaneet hankintansa omalle IT-alueelleen. IT-alueilla on omia MPLS-verkkoja, jotka on sidottu KIRKKO-verkkoon solmukohtien kautta. Yhteydet KIRKKO-verkkoon menevät IT-alueiden omien konesalien tai kytkentäpisteiden kautta. IT-alueiden omista MPLS-verkoista liikenne reitietään osittain KIRKKO-verkkoon. IT-alueilla on myös omia alueverkkoja, joita ei ole liitetty KIRKKO-verkkoon.

KIRKKO-verkon ydin on verkkoratkaisu, joka perustuu KIRKKO-verkon runkoratkaisuun [2]. Runkoratkaisulla tarkoitetaan operaattorin toimittamaa KIRKKO-verkon runkoverkkoa eli tietoliikenneverkon ydintä, joka yhdistää tietoliikenneverkkojen solmupisteet toisiinsa. KIRKKO-verkon ydin on operaattorin valvoma. Sopimus ytimen toimittamisesta on toistaiseksi voimassa oleva, mutta vanha. ydin on kirkkohallituksen hallinnassa, mutta ytimen verkkolaitteistoa ylläpitää operaattori. Kuva 1 on kuva nykyisestä KIRKKO-verkon ytimestä.



Kuva 1 KIRKKO-verkon ydin

Melkein kaikki KIRKKO-verkossa menevä liikenne menee KIRKKO-verkon ytimen läpi. Ytimen läpi menevään liikenteeseen kuuluu kaikki kahden KIRKKO-verkko liittymän välinen liikenne ja KIRKKO-verkon ja julkisen verkon välinen liikenne.

IT-alueiden alueverkkototeutuksissa liikenne ohjataan julkiseen verkkoon. Alueverkon sisäinen liikenne ei kulje KIRKKO-verkon ytimen läpi, mutta alueverkosta julkiseen verkkoon menevä liikenne kulkee ytimen lävitse. Kyseisistä alueverkoista on vain yksi liitäntä KIRKKO-verkkoon. Kirkon yhteiset VPN-ratkaisut kulkevat ytimen lävitse. VPN-tunnelin takana olevat laitteet, jotka käyttävät palveluntarjoajan konesalissa sijaitsevia palveluita, eivät kuljeta informaatiota KIRKKO-verkon ytimen lävitse. Kaikki liikenne kulkee KIRKKO-verkossa sijaitsevien virtuaalipalomuurien lävitse, joita KIRKKO-verkossa on kaksi. KIRKKO-verkko on hajautettu toteutus. Tämä tarkoittaa, että KIRKKO-verkkoon on useampi liitäntäkohta.

Kartoituksessa pääasiallisesti etsittiin kaupallisten toimittajien ja seurakuntatalouksien liitäntöjä KIRKKO-verkkoon, kuten myös IT-alueiden liitäntöjä ja sopimuksia eri toimittajien kanssa. Kartoitusprosessi pääasiallisesti hoidettiin haastatteluilla, sillä dokumentaatiomateriaali kartoitukseen liittyen ei ole julkista. Kyseinen dokumentaatiomateriaali ei ole ollut käytettävissä tätä tutkimusta tehdessä.
Kartoituksessa otettiin huomioon seurakuntaliittymien määrät IT-alueisiin, nopeudet, operaattorit, laitteisto ja IT-alueiden tarjoamat palvelut. Operaattoreiden ja laitteiston kartoitus koskevat vain IT-alueita mutta eivät toimittajia. Muut edellisissä kohdassa mainitut kartoituksen osa-alueet koskevat toimittajia ja IT-alueita.

Kartoituksessa ei otettu huomioon IP-osoitteita, sillä kartoituksen tarkoituksena on saada kokonaiskuva KIRKKO-verkosta, eikä IP-osoitealtaiden yksilöinti täl-

löin ole tarpeellista. Kartoituksessa ei myöskään ole otettu huomioon seurakuntien liitäntätapoja KIRKKO-verkkoon. Satojen yksittäisten seurakuntien laitteistojen kartoitus on miltei mahdotonta ja tarpeetonta projektin kannalta.

Sekä tässä tehdyn suurin ongelma että tulevien kartoitusten kohdalla on informaation kerääminen eri IT-alueilta. Kirkon hallintorakenteen takia yhdellä toimielimellä tai viranhaltijalla ei ole oikeutta määrätä kokonaisuuksista. Kartoitusta tehtäessä voidaan kuitenkin vedota kirkon tietoturvamääräyksiin. Kirkon tietoturvamääräykset 2.1 kohta 2, kirkkohallitus voi IT-alueiden kanssa laatia laajan katsaukset liitännöistä ja laitteistoista, jotka on liitetty KIRKKO-verkkoon**.** Tämä mahdollistaa kattavan kartoituksen KIRKKO-verkosta. Kirkkohallitus ei voi kuitenkaan antaa määräyksiä seurakunnille mitkä koskevat muutoksia, ellei kirkkolaissa anneta tähän valtuutusta. IT-alueet saavat vapaasti hoitaa KIRKKO-verkon ulkopuolella toimivat laitteistot kuten parhaaksi näkevät ja näistä laitteistoista ja liitännöistä omiin alueverkkoihin ei ole pakollista antaa tietoa kirkkohallitukselle. Kirkon autonomiasta johtuen vain kirkolliskokous voi ehdottaa kirkkolain muutosta, jonka eduskunta voi ainoastaan hyväksyä tai hylätä.

2.1 IT-alueet

Kirkkoon kuuluu noin 400 seurakuntaa, joista jokainen seurakunta kuuluu yhteen neljästätoista IT-alueesta. Jokaista IT-aluetta johtaa isäntäseurakuntatalous, jolla on tarpeeksi resursseja hoitaa IT-aluetoimintaa. Seurakuntatalouksia on kokonaisuudessaan 266. Seurakuntatalous on seurakunta, jolla on itsenäinen talous tai seurakuntayhtymä. Suurissa kaupungeissa on yleensä useita seurakuntia, jotka muodostavat yhdessä seurakuntayhtymän. Seurakuntayhtymässä hoidetaan muun muassa talous- ja henkilöstöasioita keskitetysti. [3.]

Vuonna 2007 alkoi hanke, joka koski sääntöuudistusta, jonka mukaan kirkonkirjat piti saada valtakunnallisiksi. IT-alueiden syntyyn johti aikaisempi säännös vuodelta 1994, jossa määriteltiin sähköisten järjestelmien käyttöönotto jokaisessa seurakunnassa. Vuoteen 1999 saakka Suomen evankelisluterilainen kirkko ja ortodoksinen kirkkokunta hoitivat väestökirjanpitotehtäviä yhdessä maistraattien kanssa. Vuoden 1999 jälkeen kirkolle jäi tehtäväksi hoitaa omien

jäsentensä jäsenrekisteri sekä syöttää järjestelmään tietoja esimerkiksi avioliiton solmimisesta ja sen yhteydessä mahdollisesti tapahtuneesta nimen muuttumisesta tai nimen antamisesta kasteen yhteydessä. Vuonna 2007 alkaneessa kirkonkirjojen uudistushankkeessa huomattiin tarve järjestäytyneeseen ICT (Information and Communication Technology) -toimintaan ja jokaisen seurakunnan piti liittyä ammatilliseen IT-alueeseen. Alun perin IT-alueita oli 16, mutta muutama alue on vuosien myötä lakkauttanut toimintansa ja liittynyt toisiin IT-alueisiin. Kuva 2 sisältää listan nykyisistä IT-alueista.

Arkkihiippakunnan IT-alue, Turku ja Pori
Rannikon IT-alue, Pietarsaari
Espoon IT-alue
Helsingin IT-alue, Helsingin yhtymä
Keskusrahaston IT-alue, Kirkkohallitus
Kuopion IT-alue
Jyväskylän IT-alue
Lahden IT-alue
Tampereen IT-alue
Keski-Pohjanmaan IT-alue, Ylivieska
Kouvolan IT-alue
Oulun IT-alue
Rovaniemen IT-alue
Vantaan IT-alue

Kuva 2 IT-alueet

IT-alueet hoitavat omien seurakuntiensa IT-toimintaa. Jokaisen IT-alueen sisällä toimii 10–50 kappaletta seurakuntia ja noin 500–2500 työntekijää. IT-alueisiin kuuluvien seurakuntien työntekijämäärät muuttuvat riippuen vuodenajasta. Kesäkautena saattaa työntekijöitä olla enemmän kuin talviaikaan.
IT-alueilla työskentelee 4–12 IT-asiantuntijaa riippuen IT-alueen koosta. Kun IT-alueet aloittivat toimintansa, oli suosituksena yksi IT-alueen työntekijä jokaista

100 työasemaa kohden. IT-alueet saavat päättää IT-alueen työntekijöiden määrän oman tarpeensa mukaan, jolloin suositellut työntekijämäärät eivät välttämättä ole tarkkoja.

Seurakunnat saavat vapaasti tehdä sopimukset haluamansa IT-alueen kanssa. Tehtävän kannalta ei ole tarpeellista tietää, mikä seurakuntatalous kuuluu mihinkin IT-alueeseen, koska seurakunnat voivat vaihtaa IT-alueita omien tarpeidensa mukaan.

IT-alueet saavat päättää, mitä palveluita he tarjoavat KIRKKO-verkon sisällä. Tämän takia KIRKKO-verkon sisällä saattaa olla paljon päällekkäistä infrastruktuuria, jota IT-alueet tarjoavat omille seurakunnilleen esimerkkinä voi mainita 14 eri DHCP (Dynamic Host Configuration Protocol) -palvelinta. DHCP-palvelimet antavat automaattisesti uudelle laitteelle IP-osoitteen sen liittyessä verkkoon.

IT-alueet tarjoavat palveluita omille seurakunnilleen. Yleisimpiin IT-alueiden palveluihin kuuluu KIRKKO-verkkoyhteyden antaminen, IT-tuki, tunnustenhallinta sekä turvatulostus- ja tiedostopalvelut. IT-alueiden palvelutarjonnassa on eroja, mutta niin sanotut ”yleiset” palvelut ovat käytössä kaikkialla. Palveluiden erot johtuvat IT-alueen seurakuntien tarpeista ja IT-alueiden käytettävissä olevasta laitteistoista. IT-alueet osittain myös hankkivat laitteistot ja kilpailuttavat sopimukset omille seurakunnilleen, mutta useissa tapauksissa seurakunnat saavat vapaasti päättää omista laitehankinnoistaan ja sopimuksistaan, jolloin vain laitteiston ylläpito ja tuki jäävät IT-alueen hoidettavaksi.

Muutamalla IT-alueella on käytössä innovatiivisia palveluita, joita mahdollisesti voitaisiin ottaa käyttöön koko Suomen evankelisluterilaisessa kirkossa. Esimerkkinä voi mainita Nettiradion ja kiinteistövalvontaverkot. Nettiradio on striimauspalvelu, jota käytetään erityisesti Keski-Pohjanmaan IT-alueella. Nettiradiota on pääsääntöisesti käytetty tilaisuuksien striimaukseen. Tämän hyödyntäminen muillakin IT-alueilla saattaisi ratkaista striimeihin liittyviä ongelmia, joita ilmeni eritysesti Covid-19-pandemian alkuaikoina. Nettiradiopalvelua voitaisiin myös käyttää koko kirkon laajuiseen tiedottamiseen. Kiinteistövalvontaverkko

on kiinteistöjen valvontaan rankennettu erillinen verkko, joka mahdollistaa valvontalaitteiston yhdistämisen erilliselle palvelimelle. Täten kiinteistövalvontaan liittyvät video- ja kuvamateriaalin lataaminen palvelimille on hoidettu tavalla, joka ei rasita yleistä verkkoa.

Useammalla IT-alueella on käytössä sama palveluntarjoaja IT-alueen verkkoratkaisuissa. Kyseinen palvelu mahdollistaa yhtenäisen hallinnan kaikille organisaation laitteille tietokoneista koko verkkoon ja mahdollistaa myös vahvistetut turvasäännökset laitteille ja verkolle. Koska moni IT-alue käyttää samaa ratkaisua, on se todettu hyväksi ja helpoksi tavaksi laajentaa IT-alueiden verkkoja. Kyseiset IT-alueiden verkot ovat osittain tai melkein kokonaan langattomia ja hyödyntävät VPN:ää. Koska samalla palvelulla on toteutettu useita verkkoratkaisuja IT-alueilla, on mahdollista käyttää heidän asiantuntemustaan, jos vastaava järjestelmä halutaan ottaa käyttöön koko kirkossa.

IT-alueet tekevät osittain yhteistyötä toistensa kanssa. Kaksi yleisintä yhteistyön kohdetta ovat SCCM (System Center Configuration Manager) ja yhteinen palvelupyyntöjärjestelmä. SCCM on laitehallintaohjelma Windows-pohjaisille tietokoneille. SCCM:ää käytetään yhteisteistyössä useamman IT-alueen kanssa, jotta laitehallinta olisi helpompaa ja halvempaa. Kaikki IT-alueet eivät kuitenkaan koe tarvitsevansa yhteistä SCCM-palvelua ja hoitavatkin laitehallinnan itse. Palvelupyyntöjärjestelmä on yhteinen myös usealla IT-alueella. Yhteinen palvelupyyntöjärjestelmä mahdollistaa kulujen laskun, kun tiketit hoidetaan keskitetysti. Kaikki IT-alueet eivät myöskään kuulu yhteiseen palvelupyyntöjärjestelmään. Yhteinen palvelupyyntöjärjestelmä saatetaan kokea turhana tai riittämättömänä IT-alueen IT-tuen yleisen tason ylläpitämiseksi. IT-tuessa on toisenlaistakin yhteistyötä. Siitä tarkemmin on IT-tuki kohdassa.

2.2 Laitteiston hankinta

Jokaisella IT-alueella on omat ratkaisut laitteiston hankintaan. Osa IT-alueista ostaa omat laitteistonsa, jotkut alueet vuokraavat ja joillain alueilla sekä ostetaan että vuokrataan laitteistoa toimittajalta omien tarpeiden mukaan. Toimittajalta vuokratut laitteistot on myös mahdollista joissain tapauksissa ostaa itselleen sopimuksen päätyttyä. Kirkkohallituksen IT-alueella käytetään jälkimmäistä vaihtoehtoa ja pyritään vuokraamaan kaikki laitteisto, jos se vain on mahdollista. KIRKKO-verkon ytimen laitteisto on vuokrattua toimittajalta. Nykyisessä laitehankintaprosessissa ei ole ongelmaa, mutta jos KIRKKO-verkko uudistetaan, pitää verkkolaitteistoa luultavasti uusia. Verkkolaitteiston uusiminen on IT-aluekohtaista, mutta oletus on, ettei kaikilla IT-alueilla ole välttämättä yhteensopivaa verkkolaitteistoa KIRKKO-verkon uudistamiseksi.

Kun puhutaan laitteistosta, sisällytetään siihen kaikki KIRKKO-verkkoon liitetyt laitteet palvelimista tietokoneisiin. Turvajärjestelmiin liitetyt laitteet ovat poikkeus, sillä niihin keskitytään omana aihealueena.

2.3 Tulevaisuuden visio

Kannattavaa tulevaisuudessa olisi saada lisää yhtenäisiä ratkaisuja IT-alueiden välillä, jotka ajaisivat KIRKKO-verkon uudistusta eteenpäin. KIRKKO-verkkoa voisi aluksi supistaa, mikä käytännössä tarkoittaisi IT-alueiden välisten erojen karsimista minimiin. Verkon supistuksen voisi aloittaa antamalla vain yhden operaattorin toimia KIRKKO-verkossa. Yhden operaattorin verkko ratkaisisi ongelmat, joita monioperaattoriverkoissa voi ilmetä.

Monioperaattoriverkko on teoreettisesti hyvä lähtökohta uuden KIRKKO-verkon pohjaksi, mutta haastatteluissa kävi ilmi, että ongelmien ilmetessä verkossa saattavat verkon ylläpitävät operaattorit kiistellä ongelman aiheuttajasta. Kiistat saattavat jatkua pitkiäkin aikoja, jolloin verkkoyhteydet eivät toimi halutulla tavalla ja aiheuttavat harmia loppukäyttäjille. Monioperaattoriverkon toteuttaminen

on myös hankalaa, koska operaattorit eivät välttämättä halua oman liiketoimintamallinsa takia tehdä yhteistyötä toisten operaattoreiden kanssa. Monioperaattoriverkot yleisesti toimivat yksittäisten sisäverkkojen sisällä (kuten sairaalat ja kerrostalot). Suuressa verkkouudistuksessa kuten KIRKKO-verkon uudistusprojektissa monioperaattoriverkon implementointi voi olla työlästä eikä haluttuja hyötyjä ei välttämättä saavuteta. Suurimpana ongelmana kuitenkin monioperaattoriverkon toteuttamiselle ovat kustannukset. Verkkouudistuksen tarkoituksena on pienentää kustannuksia ja parantaa KIRKKO-verkkokokonaisuutta. Monioperaattoriverkon implementointi tarkoittaisi kirkolta lisäkustannuksia laitteiden ja laitehallinnan kannalta, koska verkkolaitteisto KIRKKO-verkon ytimeen oletettavasti pitäisi tehdä omana hankintanaan.

Supistuksen yhteydessä voisi myös ottaa käyttöön yhteisiä käytäntöjä IT-alueiden välillä, joissa sovitaan samojen ohjelmien ja palvelimien käytöstä. IT-alueet saisivat vielä kuitenkin tarjota omia palvelujaan seurakunnilleen kuten aikaisemminkin. Laitteiden hallinta helpottuisi samalla, koska ongelmien ratkaisuun voisi liittyä kaikkien IT-alueiden asiantuntijat. On otettava huomioon, että nykyisessä järjestelyssä jokaisella IT-alueella on omat toimintatapansa käytössä, ja suuret muutokset saattavat saada negatiivisen vastaanoton, jolloin yhteisten linjauksien muutos tulisi aloittaa pienillä muutoksilla.

KIRKKO-verkon voisi tulevaisuudessa toteuttaa kokonaan langattomana verkkona. Langattoman verkon käyttöönottoon vaikuttavat myös operaattoreiden viimeaikaiset suunnitelmat luopua kuparikaapelien käytöstä kokonaan. Uusien kaapelointien hankkiminen saattaisi maksaa huomattavasti enemmän kuin langattoman verkon implementointi. Langattomien 4G-verkkojen vahvuudet ovat hallinnan helppous, joustavuus, nopea asennusaika ja riippumattomuus fyysisistä kaapeleista, jolloin verkon toiminta-aika (Up-time) paranee. 4G-verkon rakentamisessa on kuitenkin omat ongelmansa. 4G-verkko kykenee 300-150Mbps:n latausnopeuteen ja 150-50Mbps:n lähetysnopeuteen, mutta nämä nopeudet ovat vain teoreettisia. Todelliset nopeudet voivat olla jopa vain 1/5 teoreettisesta nopeudesta. Suuret nopeuden muutokset johtuvat verkkoon kohdistuvasta liikenteen määrästä tai vastaanottimien maantieteellisestä sijainnista.

KIRKKO-verkon virtualisoinnissa tuleekin ottaa huomioon mahdolliset ongelmat 4G-yhteyksien nopeuksissa. Langattomissa yritysverkoissa vielä toistaiseksi hyödynnetään 4G-yhteyksiä, mutta 5G-yhteydet yleistyvät suomessa ja täten 5G-valmiudet kannattaa implementoida koko verkon laajuisesti. Verkkouudistuksen kilpailutusvaiheessa operaattoreilta kannattaakin kysyä, mihin alueisiin 5G-verkko jo nyt voidaan implementoida. Koska 5G-verkko ei vielä ole koko maan kattava, pienemmillä paikkakunnilla joudutaan käyttämään 4G-yhteyksiä.

KIRKKO-verkon muuttaminen virtuaaliverkoksi olisi kannattavaa. Virtuaaliverkkoratkaisua on helppo kontrolloida ja käyttää, eikä se ole suoranaisesti sidottuna tiettyyn paikkaan. Isossa organisaatiossa, kuten Suomen evankelisluterilainen kirkko, toimistorakennukset ja muut työskentelypaikat vaihtuvat usein, jolloin virtuaaliverkko kulkisi mukana ja olisi helppo asentaa toimintakuntoon paikan vaihtuessa. Nykyisessä järjestelyssä fyysiset kaapeloinnit hidastavat toimitilavaihdoksia, koska uudessa toimitilassa ei välttämättä ole fyysisiä kaapelointeja valmiina tai laitteet joudutaan uudelleen konfiguroimaan muuton yhteydessä. Langattomat ratkaisut pystyvät korvaamaan kuparikaapeliyhteydet eri paikkakunnilla. On mahdollista, että osassa pienimmistä paikkakunnista langattoman verkon kuuluvuus voi olla odotettua huonompaa, mutta sitä voi yksittäisillä alueilla korjata esimerkiksi vahvistinantennien avulla.

Langaton verkko tulee kahdentaa käytön yhteydessä, jotta pystytään varmistamaan yhteyksien toiminta laitevioista tai muusta ongelmasta riippumatta. Uuden verkkolaitteiston tulisi siis olla sopivaa verkon moitteettoman toiminnan kannalta. Laitteistoon kannattaa harkita niin sanottuja All in One -verkkolaitteita ainakin alkuimplementoinnin yhteydessä, koska ne mahdollistavat langattomat yhteydet ja kiinteät yhteydet samanaikaisesti samalla laitteella, jolloin riskit yhteyksien katkeilussa minimoidaan.

Langattoman verkon käyttöönoton yhteydessä kannattaa ottaa käyttöön myös SD-WAN (Software-defined Wide Area Network) -verkkoratkaisu. SD-WAN on palvelu, jonka avulla pystyy kontrolloimaan liikennettä turvallisesti ja tehokkaasti

WAN:in (Wide Area Network) sisällä. SD-WAN-ratkaisu voi hyödyntää kaikkia yhteystapoja. Tämä tarkoittaa, että yksittäiset toimipisteet voivat käyttää rinnakkain eri yhteyksiä kuten MPLS-yritysverkkoa, langattomia verkkoja tai internetliittymiä. SD-WAN kykenee myös älykkääseen liikenteen ohjaukseen ja aktiiviseen kuormanjakoon. Nämä ovat oleellinen osa jokaista suurta verkko infrastruktuuria, koska ne parantavat verkon kokonaista vikasietokykyä ja mahdollistavat paremman toiminnan jatkuvuuden. SD-WAN mahdollistaa myös keskitetyn hallinnan verkon ylläpitäjille. On huomioitava, että mahdollisimman korkean tietoturvatason saavuttamiseksi SD-WAN kannattaa ottaa käyttöön heti uudistuksen alkaessa. Erillisten palomuurien rakentaminen jälkeenpäin saattaa osoittautua vaikeaksi ja nostaa lisäkustannuksia huomattavasti. [4.] SD-WAN ei myöskään ole riippuvainen operaattorista, mikä kirkon tilanteessa on erittäin hyödyllistä, koska jokaisella IT-alueella on päätösvalta tehdä omat operaattorisopimuksensa ja kirkon tulee noudattaa julkisena toimijana kilpailutusta koskevaa lainsäädäntöä. Nykytilanteessa IT-alueilla on omat sopimukset eri operaattoreiden kanssa ja uudistuksen yhteydessä SD-WAN mahdollistaisi verkon uudistamisen operaattoreista ja verkkoliitäntätavoista riippumatta. SD-WAN:ista on jo kokemusta yhdellä IT-alueista ja kyseiseltä IT-alueelta kannattaa kysyä SD-WAN-verkkoratkaisun implementoinnista muihinkin IT-alueisiin.

Korkean tietoturvatason ylläpitämiseksi langattomassa verkossa on mahdollista myös implementoida rinnakkaisverkko (parallel network) tai niin sanottu ”ilmaväli” (air-gapping). Tällä tarkoitetaan langattoman verkon rinnalle tehtyä erillistä rinnakkaisverkkoa, jonka sisällä olevat laitteet ovat erillään riskialttiista verkosta kuten julkinen verkko. Rinnakkaisverkosta ei voi liittyä julkiseen verkkoon, mutta kirkon mahdolliset varmuuskopiot löytyvät omasta eristetystä verkosta, jos omalle varmuuskopiointipalvelimelle nähdään tarvetta. Rinnakkaisverkon tarkoituksena on tietoturvan ylläpitäminen ja minimoida mahdollisten tietoturvamurtojen määrää. Rinnakkaisverkon sisällä olevilla koneilla ei kuitenkaan voida hoitaa työtehtäviä, joihin tarvitaan yhteys julkiseen internetverkkoon, koska nämä tietokoneet ovat fyysisesti erotettu muista verkoista. [5.] Kyseisen verkon rakentaminen ei kuitenkaan ole välttämättä tarpeellista kirkolle, mutta se on yksi

mahdollisuus, jos tulevaisuudessa nähdään tarvetta aiempaa tiukemmalle tietoturvalle.

3 Laitehallinta

Kirkolla on noin 12 000 työasemaa ja noin 15 000 käyttäjää. Laitehallintaan liittyvissä uudistuksissa tulee ottaa huomioon eri IT-alueiden tarpeet. Tällä hetkellä IT-alueet pääasiallisesti hoitavat oman alueensa laitehallinnan. Tässä voi olla poikkeuksia kuten Espoo ja kirkkohallitus, joiden laitehallinta on samanlainen. Laitehallintaa hoidetaan MEM (Microsoft Endpoint Manager) -ohjelmalla, jonka avulla pystytään määrittämään laitteistoille erilaisia sääntöjä, asetuksia ja dynaamisiaryhmiä, joihin tietyt säännöt ja asetukset liitetään. Asetukset ovat ryhmä sääntöjä, jotka on viety pilveen. Muutamalla IT-alueella on käytössä yhteisiä sääntöjä laitehallinnassa. Monella IT-alueella on käytössä vanhoja laitehallinnan sääntöjä, joita luultavasti on muokattu ajan myötä. Ryhmäsäännöistä puhuttaessa tarkoitetaan asetuksia. Toisin sanoen, jos kyseinen ryhmäsääntö viedään pilveen, kyseessä on asetus.

Kun puhutaan laitehallinnan laitteistosta, kuuluu siihen pääosin työtietokoneet ja työpuhelimet. Henkilökohtaiset laitteet voidaan myös lisätä laitehallintaan, mutta tällöin hallintaprosessi muuttuu, sillä samoja sääntöjä työlaitteiden kanssa ei voida käyttää. Suurin osa seurakuntien laitteistosta on Windows-pohjaisia ja laitehallinta onkin pääosin suunniteltu näitä laitteita varten. Applen laitteita kyetään tällä hetkellä myös rajoitetusti hallitsemaan. Applen laitteisto tarvitsisi oman hallintajärjestelmänsä, jolloin kyseisen järjestelmän käyttöön ottaminen toisi lisäkustannuksia. Yleisesti IT-alueet pyrkivät tämän syyn takia käyttämään Windows-pohjaista laitteistoa.

Puhelimissa on käytössä Intune, joka on pilvipalveluratkaisu puhelimiin liittyvässä laitehallinnassa. Intune mahdollistaa puhelimien ohjelmien hallinnan MAM (Mobile Application Management) ja puhelimien laitehallinnan MDM (mobile device management) [6]. MAM-puolella voitaisiin hoitaa henkilökohtaisia

laitteita, mutta MAM-puolta ei ole otettu käyttöön, koska se tuottaisi liikaa ongelmia nykyisen laitehallinnan kannalta. MAM on pääasiallisesti suunnattu henkilökohtaiseille laitteille, joten ei ole perustetta ottaa sitä käyttöön, varsinkin jos työnantaja tarjoaa laitteet. Henkilökohtaisia Applen laitteita käsitellään puhelimina tällä hetkellä, mikä merkitsee, ettei kyseisillä laitteilla pääse esimerkiksi Kirjuri-järjestelmään, mutta niillä pystyy käyttämään Officen ohjelmistoa ja hoitamaan perustyötehtävät. MAM vaatii applikaatiosuojauksen ja DLP:n (data loss prevention tai data leak prevention), mikä vaatii lisenssejä. DLP:n tarkoitus voi muuttua riippuen, puhutaanko datan menettämisestä vai datan vuotamisesta ulkoiselle tekijälle. Koska MAM vaatisi DLP:n, merkitsisi tämä uusien lisenssien hankintaa, ja täten kulut nousisivat.

.

3.1 Säännöt ja dynaamiset ryhmät

Säännöt ovat asetuksia laitehallinnassa, joiden avulla hallitaan työlaitteistoa (tietokoneet ja puhelimet). Osa säännöistä on otettu yleisesti käyttöön, kuten tietokoneiden kyky keskustella keskenään. Tämä mahdollistaa päivitysten latauksen naapurikoneelta, jos kyseinen naapurikone on päivitetty. Tällöin tietokoneiden päivitysten lataaminen on tehokasta, eikä jokaisen päivityksen kohdalla tarvitse latausta hankkia internetin kautta.

Muihin yleisiin sääntöihin voi lajitella Wlan-säännöt, joiden avulla saa yhteyden paikallisiin Wlan-verkkoihin IT-alueen ulkopuolisista työpisteistä. Yleiset Wlan-säännöt ovat käytössä kirkkohallituksessa, Helsingissä, Espoossa ja Jyväskylässä. Muilla IT-alueilla saattaa olla Wlaniin omat säännöt. Wlan-säännöille on olemassa yhteinen sääntöluokka, mutta sitä ei toistaiseksi ole otettu yleisesti käyttöön. Wlan-sääntöjä ei viedä pilveen. Wlan-sääntöjen vienti pilveen vaatisi PEAP:n (Protected Extensible Authentication Protocol), jonka sertifikaattipohjaiselle käsittelylle ei ole mahdollisuutta. PEAP on todennusprotokolla, jota käytetään muun muassa langattomissa verkkoyhteyksissä.

Dynaamiset ryhmät ovat laitehallinnassa ryhmiä, joiden avulla voidaan päivittää automaattisesti ryhmään kuuluvien jäsenten lisenssi ja ohjelmistoon liitettäviä käyttöoikeuksia. Dynaamiseen ryhmään jäsenet liittyvät automaattisesti tietyn ominaisuuden (attribute) perusteella. Ominaisuus voi olla ohjelma tai tietyn ohjelman käyttöoikeuksien määrittely, jonka käyttöön käyttäjä tarvitsee luvan laitehallinnasta. Saatuaan pyynnön laitehallinnan työntekijä voi lisätä ominaisuuden käyttäjän tiliin, jolloin tieto latautuu pilveen ja pilven kautta dynaamiseen ryhmään. Dynaamiset ryhmät osaavat automaattisesti lukea ominaisuuksia ja täten lajitella tietyn ominaisuuden omaavat käyttäjät oikeisiin ryhmiin.

3.2 Ohjelmisto

Tällä hetkellä kirkon ohjelmistoon kuuluvat vakiona Microsoft Office 365 (O365), Desktopinfo, acrobat reader, java, winzip, vmi provider (sarjanumerot näytöistä). Muitakin ohjelmia saa asennettua työkoneelle, jos sille on tarvetta, mutta käyttäjä tarvitsee ohjelmien asentamiseen luvan IT-tukihenkilöstöltä ja ohjelman tulee olla hyväksytty Software Centeriin. Työntekijät voivat lähettää IT-tukeen tikettejä, joissa pyytävät lisäohjelmistoja Software Centeriin. Ohjelman hyväksyminen vaatii, että EULA (End-user License Agreement) eli loppukäyttäjän lisenssisopimus [7] on kunnossa ja lisättävä ohjelma on työnteon kannalta hyödyllinen tai pakollinen sekä tietoturvallinen. Ohjelman lisäämiselle tulee olla hyvä perustelu. Ohjelmiston lisäystä voi pyytää kaikki kirkon työntekijät, mutta IT-alueen tietohallintopäällikkö päättää, onko kyseinen ohjelma tarpeellinen ja täyttääkö se tarvittavat tietoturvaan liittyvät kriteerit.

3.3 IT-tuki

Keskusrahaston IT-alueen IT-tukeen tulee noin 21 200 palvelupyyntöä vuodessa, joista puheluja noin 5700 kpl ja tikettejä noin 15 500. Yleensä palvelupyynnöt lisääntyvät vuosittain. Kyseisellä IT-alueella on noin 1500 työntekijää ja

reilut 100 toimipistettä. Yleisesti IT-alueet hoitavat omien seurakuntiensa tukipyynnöt. Erona muihin IT-alueisiin Keskusrahaston IT-alue hoitaa valtakunnallisen tuen 5 eri ohjelmaan, joita ovat jäsentietojärjestelmä Kirjuri, asianhallintajärjestelmä Domus, taloushallintojärjestelmä Status, nettisivunjulkaisujärjestelmä Lukkari ja M365. Keskusrahaston IT-tuki hoitaa tavanomaista suurempien käyttäjäoikeuksien tarvitsemiseen liittyvät tehtävät. Tällaisessa tilanteessa keskusrahaston tuki toimii IT-tukena muiden IT-alueiden IT-tuelle. Näitä pyyntöjä käsitellään keskusrahaston IT-tuessa harvoin. Tämänhetkinen IT-tukijärjestely on kustannustehokasta.
IT-tukea tarjotaan käytännössä pelkästään Windows-työkoneille. Applen koneille ei tällä hetkellä omaa tukea löydy, sillä Applen laitteiden käyttö on kirkossa vähäistä. Jos kuitenkin Applen laitteistoa haluttaisi tulevaisuudessa ostaa tai ottaa enemmän käyttöön, vaatisi se lisää osaavia työntekijöitä ja oman IT-tuen, jolloin kustannukset nousisivat jokaisella IT-alueella.

Operaattorit hoitavat oman IT-tuen, sillä koko verkon hoitamiseen tarvittavaa tukea kirkolta ei löydy. Toimittajat hoitavat omat tukensa kaikissa tarjoamissaan palveluissa (ulkopuolelta hankitut palvelut 3. tason tuki on toimittajalla).

IT-tukea hoidetaan IT-alueilla eri tavoin. IT-alueet tarjoavat IT-tukea pääsääntöisesti etänä, mutta lähitukea on myös tarvittaessa saatavissa. Lähitukea tarjotaan tilanteissa, joissa on välttämätöntä päästä seurakunnan tiloihin. Lähitukitapauksiin kuuluvat muun muassa laitteistohuollot ja vaihdot. IT-alueet ovatkin usein jakaneet maantieteellisesti suurilla IT-alueilla työntekijöitä useampaan paikkaan. Työntekijöiden sijoittaminen IT-alueen eri osiin mahdollistaa lähituen helpommin, sillä matkat saattavat olla pitkiä seurakuntien välillä, jolloin aikaa ja matkakuluja säästetään taktisella työntekijöiden sijoituksella. IT-alueet hoitavat pääasiallisesti itse lähitukensa. Rannikon IT-alueen ja kirkkohallituksen lähituki on ulkoistettu. Ulkoistus rannikon IT-alueella johtuu maantieteellisestä sijainnista. Rannikon IT-alueeseen kuuluu Ahvenanmaa ja muuta saaristoa. Näihin paikkoihin on vaikea päästä hoitamaan lähitukitehtäviä, joten ulkoistaminen on käytännössä ainoa järkevä tapa hoitaa tuki.

IT-alueilla pääsääntöisesti hoidetaan kaikki IT-tukeen liittyvät asiat itsenäisesti. Muutama IT-alue kuitenkin tekee yhteistyötä keskenään. Kannattava esimerkki IT-tuen yhteistyöstä on Lahden IT-alueen ja Keski-Suomen IT-alueen välisestä sopimuksesta, jonka tarkoituksena on varmistaa IT-tuen toiminta tilanteissa, joissa toisen IT-alueen työntekijät eivät pystyisi hoitamaan työtehtäviään. Esimerkkinä on Covid-19-pandemia, joka saattaa lamauttaa yhden IT-alueen kokonaan, jos IT-alueen työntekijät sairastuisivat samanaikaisesti. Tällaista järjestelyä kannattaa harkita muillakin IT-alueilla, jotta pystytään varmistamaan käyttäjien IT-tuki, vaikka yksi IT-alue hetkellisesti saattaisikin lamautua. Toisena vaihtoehtona on ulkoistaa IT-tuki, mutta kyseinen järjestely saattaa aiheuttaa vastustusta ja vaatisi lainsäädännön mukaista kilpailutusta. IT-tuen ulkoistaminen ei välttämättä kuitenkaan nosta kustannuksia, mutta voisi huonontaa asiakaspalvelua joillain IT-alueilla.

3.4 Laitehallinta uudistuksen myötä

IT-alueet voisivat aloittaa keskustelut laitehallinnan yhtenäistämisestä. Tarkoituksena ei ole ottaa laitehallintapuolta pois IT-alueilta vaan luoda paremmin tuettu laitehallinta niin sanottuja ”kriisitilanteita” varten. IT-alueiden tulee ottaa huomioon erikoisolosuhteet ja täten yhtenäisen laitehallinnan tutustuttaminen kaikille IT-alueille olisi kannattavaa. Normaaliolosuhteissa IT-alueet saavat tulevaisuudessakin hoitaa omaan laitehallintaan liittyvät työtehtävät, mutta mahdollisten ongelmien ilmetessä muut IT-alueet voivat avustaa laitehallinnassa ja täten tasata työkuormaa yksittäisiltä IT-alueilta. Uudistuksen voi aloittaa yksittäisten IT-alueiden keskinäisillä sopimuksilla, mutta kuitenkin luoda yhtenäinen laitehallintapohja kaikkien IT-alueiden välille.

Laitehallinnassa voitaisiin lisätä dynaamisten ryhmien käyttöä. Dynaamisilla ryhmillä voitaisiin helpottaa laitehallintaan liittyvien ohjelmien ja lisenssien lupien myöntämistä pyyntöjen hyväksymisen yhteydessä. Ladattaville lisäohjelmille voitaisiin luoda omat ryhmät, johon luvan saaneet käyttäjät lisätään. Kun luvan saanut käyttäjä on lisätty ryhmään, saa käyttäjä automaattisesti luvan ladata

pyytämänsä ohjelman koneelleen ja mukana tulee ohjelman käyttöön tarvittava lisenssi. Tällä hetkellä ohjelmien latausoikeus ja lisenssi annetaan erikseen, ja tämä saattaa tuottaa useiden tuntien viivästymisen työnteossa.

IT-alue kohtainen SSID voitaisiin lisätä yhteisiin sääntöihin, jolloin koko maassa voitaisiin kirjautua sisään Wlaniin automaattisesti missä päin Suomea tahansa. Tämä yhteissääntöluokka Wlanille ei itsessään ole merkittävä muutos, mutta esimerkiksi työmatkoilla sääntö helpottaisi töiden tekemistä oman IT-alueen ulkopuolella.

4 Pilvipalvelut

Tällä hetkellä kirkossa pääasiallisesti käytetään Azuren pilvipalvelualustaa. IT-alueiden kannattaisikin välttää muiden alustojen käyttöä. Käyttöoikeuksien hallinta olisi paljon helpompaa, jos kaikki IT-alueet olisivat samassa tenantissa (Tenant). Tällä hetkellä kirkolla on Azuressa useampi tenantti käytössä ja näiden hallinta on tenantin omistavan IT-alueen vastuulla. Tenantti on yksittäinen tili, joka sisältää kaikki organisaation käyttäjät, tilaukset ja domainit. Yhdessä tenantissa on mahdollista olla useampi domain. [8.] Domain on verkkotunnus.

Pilvipalveluiden käyttö lisääntyy jatkuvasti IT-alueilla ja tähän liittyen olisi kannattavaa tehdä yhteinen linjaus IT-alueiden välillä, jotta pilvipalveluiden hallinnasta ei tulisi tarpeettoman monimutkaista ja kaikille IT-alueille löytyisi oma sopiva tapa hoitaa pilvipalveluihin liittyvät asiat.

4.1 Azure

Kirkko käyttää Azuren pilvipalveluita, mutta niiden käyttö on kuitenkin vähäistä. Suurin osa Azureen liittyvistä palveluista on käytössä pääkaupunkiseudulla, etenkin kirkkohallituksessa. Muilla IT-alueilla Azuren käyttö on lisääntynyt, ja osa IT-alueista yrittääkin hyödyntää tulevissa uudistuksissaan pilvipalveluita

mahdollisimman paljon. Azuren käyttöä lisäävät IT-alueet pyrkivät hyödyntämään pilvipalvelualustaa muun muassa dokumenttien käsittelyssä (tallennus/jakaminen), tulostuspalveluissa ja yleisesti ohjelmistojen käytössä.

IT-alueet voivat halutessaan tilata itselleen kirkkohallituksen omistuksessa olevan tenantin. Tämä mahdollistaa omien resurssiryhmien tekemisen, joita IT-alueet voivat käyttää omiin tarpeisiinsa. Laskutus hoidettaisiin tällöin käytön mukaan. Tämä aiheuttaa IT-alueille omat ongelmansa Azuren käytössä. Koska yksi käytössä oleva tenantti on kirkkohallituksen hallinnassa, saattaa olla haasteellista saada houkuteltua muut IT-alueet liittymään kirkon Azure-pilveen. Azuren pääkäyttäjät ovat kirkkohallituksen työntekijöitä, mutta IT-alueet voisivat liittyessään Azureen hallita omia perustoimiaan pilvessä. Kiistaa saattaakin syntyä korkeimmista Cloud admin-oikeuksista. Lainsäädännölliset ongelmat Cloud admin-oikeuksien antamisesta estää niiden jakamisen muille käyttäjille. Jotkut IT-alueista ovat hankkineet oman tenantin Azuresta tai saattavat harkita oman tenantin hankkimista. Omien tenanttien hankkiminen ratkaisee kiistat hallinnan kannalta, mutta samalla luo suurempaa eriytymistä yhteisestä kokonaisuudesta. Tulevaisuuden kannalta IT-alueiden omat tenantit ovat tarpeeton ylimääräinen kuluerä.

KIRKKO-verkkoa on jatkettu Azureen. Kyseessä on VPN-putken kaltainen ratkaisu, jonka avulla yhdistetään KIRKKO-verkko ja Azuren verkko. Tämä toteutetaan Expressroutella. ExpressRouten avulla pystytään jatkamaan paikallisia verkkoja Microsoftin pilveen käyttämällä privaattia internetyhteyttä. [9.] ExpressRoute on luotettavampi ja helpommin hallittavissa kuin VPN, koska ExpressRoutea käyttävä liikenne ei kulje julkisen verkon kautta.

Microsoft tarjoaa valmiina alueittain kahdennetut palvelinpaikat. Kahdentamisella tarkoitetaan tallennettavien materiaalien ja palveluiden varmentamista kahdelle tai useammalle eri palvelimille, jolloin palvelut ja tallennetut tiedostot ovat käytössä, vaikka yksi palvelin vahingoittuisi tai ei jostain toisesta syystä olisi käytettävissä. Tämä mahdollistaa, että Microsoftin palvelimet on kahden-

nettu asiakkaan valitseman alueen mukaan. Esimerkiksi kyseessä voi olla Pohjois-Eurooppa, jolloin palvelinalustat on kahdennettu Pohjois-Euroopassa sijaitseviin Microsoftin palvelimiin.

4.2 Muut pilvipalveluasiat

Uusien pilvipalvelualustojen hankkiminen on toistaiseksi tarpeetonta. On mahdollista, että toisilta palvelualustojen tarjoajilta saisi tiettyihin tehtäviin paremmin soveltuvia ohjelmistoja, mutta uusien alustojen lisääminen tarvitsisi lisää osaavia työntekijöitä, jolloin kustannukset nousisivat alustan sekä alustan hankinnan, että lisähenkilöstön tähden. Tulee ottaa myös huomioon, että kokonaisuuksien hallitsemisesta tulisi monimutkaisempaa, jos käytössä on useampi pilvipalvelualusta.

Vaikka tällä hetkellä ei ole tarvetta hankkia muita pilvipalvelualustoja, on silti kannattavaa seurata muiden pilvipalveluiden tuotetarjontaa. On mahdollista, että tulevaisuudessa etätöiden lisääntyessä ja teknologian kehityksen mukana tulevat uudet tekniset ratkaisut pystytään saamaan tehokkaammin ja paremmin toisilta pilvipalvelun tarjoajalta. Käyttöönottamisessa tulee ottaa huomioon useamman pilvipalvelualustan ongelmat, kuten lisäkustannukset, käytettävyys ja hallintaprosessien toiminta.

Kirkon käyttämiin pilvipalveluihin kannattaa tehdä yhteiset linjaukset. Azure on ainoa realistinen vaihtoehto tällä hetkellä. Kannattavaa on kuitenkin, jos uusia pilvipalvelualustoja hankitaan, pitää alustat yhteisinä helpon hallinnan kannalta. Yhteiset käytännöt, alustat ja sovellukset avustaisivat tulevissa kartoituksissa, jos uudelleen kartoittamiselle on tarvetta ja yhteisten ohjelmistojen ja laitteiden hallinta helpottuisi samalla, koska ongelmien ratkaisuun voisi liittyä kaikkien IT-alueiden asiantuntijat.

Kirkossa voitaisiin sopia yhteisen pilvipalvelualustan käytöstä, jolloin hallinta-prosesseissa ei syntyisi ristiriitoja, kun pilvipalvelujen käyttö lisääntyy. Pilvipalveluiden lisääntymisen yhteydessä kannattaa huomioida kaikkien IT-alueiden tarpeet ja pitää keskustelu avoimena. Kaikille IT-alueille sopiva yhteinen hallintajärjestelmä olisi optimaalista, sillä se lisäisi tehokuutta ja tulevaisuudessa uudistuksien yhtenäistä käyttöönottoa.

Nykyistä laajempiin pilvipalveluihin liittyy myös riskejä. Niihin kuuluvat muun muassa käyttökatkokset, jotka eivät johdu Suomen tai kirkon hallitsemista laitteista ja verkkoyhteyksistä. Usein pilvipalveluiden palvelimet ovat Suomen rajojen ulkopuolella, ja täten ulkomailla tapahtuvat laiteviat tai kriisit voivat suoranaisesti vaikuttaa Suomessa oleviin organisaatioihin. Toinen huomioon otettava asia on tietoturva. Nykyisyydessään esimerkiksi kirjuriin liittyvää tietoa ei saa viedä suomen rajojen ulkopuolelle, mutta kannattavaa on myös harkita, mitä muita asioita ei välttämättä kannata ulkomaiden tarjoamille palvelimille viedä. IT-alueet saavat itse päättää, kuinka he haluavat hoitaa omiin pilvipalveluihinsa liittyvät tietoturva-asiat, kunhan päätökset ovat lain mukaisia.

Kirkolla on koko maanlaajuisesti käytössä Microsoft 365 (M365) -palvelu, johon sisältyy Office 365:den lisäksi Microsoftin lisenssit kuten Windows käyttöjärjestelmän lisenssi. M365-palvelua tarvitaan, sillä kaikki työnantajalta saadut koneet käyttävät Windowsin käyttöjärjestelmää. Kirkolta saa omalle henkilökohtaiselle tietokoneelle M365-lisenssin tarvittaessa käyttämällä omaa z-tunnusta eli kirkon antamaa käyttäjätunnusta, mutta lisenssi lakkaa toimimasta, kun työsuhde loppuu ja z-tunnus deaktivoidaan.

Kaikilla seurakunnilla on tällä hetkellä käytössä O365-ympäristö. O365 on Microsoftin tarjoama pilvipalvelu, jonka avulla pystytään helpottamaan työskentelyä ryhmissä yritysten tai organisaatioiden sisällä. O365-palveluun kuuluu Office-paketin ohjelmat Word, Powerpoint, Excel tunnetuimpina, mutta palveluun kuuluvat myös sähköposti, kalenteri, Microsoft Teams ja OneDrive, minkä avulla voidaan tallentaa tiedostoja pilveen ja jakaa niitä muille.

5 Kirjuri

Kirjuri on jäsentietojärjestelmä. Kirjuri mahdollistaa oikeudet saaneita työntekijöitä katsomaan ja muokkaamaan kirkon jäsenten tietoja jäsentietojärjestelmässä. Tiedot järjestelmän sisällä ovat salassapidettäviä, sillä kyseisestä järjestelmästä löytyy kirkon jäsenten henkilökohtaiset tiedot, kuten sotu, sukulaissuhteet ja osoitetiedot. Kirjuria esimerkiksi käytetään esteiden tutkinnassa (aviovliitto), perun kirjoitusta varten annettavissa todistuksissa, kasteessa, kummikelpoisuuden tutkimisessa, sukuselvityksissä ja kirkkoon liityttäessä. Jäsentietojärjestelmää voidaan hyödyntää myös viestinnässä.

Kirjurilla on oma toimittaja. Täten järjestelmään liittyvien ongelmien ratkaisijana toimii toimittajan IT-tuki. Käyttöön liittyviä ongelmia ratkaisevat IT-alueet, kirkkohallituksen tietohallinto tai kirjurin oma IT-tuki. Kirjurin palvelimet on hankittu erilliseltä toimittajalta, ja täten palvelimiin liittyvät huollot ja ongelmien ratkaisut hoitaa toimittaja.

Kirjurin käytössä vaaditaan monivaiheista tunnistautumista (multifactor authentication, MFA). Tällä tarkoitetaan käyttäjätunnuksen ja salasanan lisäksi toista tunnistautumistapaa, joka voi olla esimerkiksi puhelin. Kirjurin tapauksessa MFA toimii tunnistautumiskorteilla puhelimen tai muun vastaavan sijaan. Kirjuriin kirjautuessa käyttäjällä tulee olla oma z-tunnus ja tunnistautumiskortti, johon tarvitsee oman PIN-koodin. Jokainen tunnistautumiskortti on henkilökohtainen, ja työsuhteen päätyttyä kortti deaktivoidaan.

5.1 Laki ja tietoturva

Kirjurin käytössä tulee noudattaa digi- ja väestötietoviraston (DVV) antamia ohjeita. Laissa annetaan tietoturvaa ja käyttöä koskevat määräykset. Henkilötietojen käsittely voi olla manuaalista tai automaattista. Käsittelytavasta riippumatta tulee noudattaa tietosuojalain määräyksiä. [10.]

Perustuslaissa määritetään, että yksityisyyden suoja on jokaisen ihmisen perusoikeus. Julkisuuslain mukaan vaitiolovelvollisia ovat työ- tai virkasuhteessa olevat henkilöt sekä myös luottamustehtäviä hoitavat henkilöt. Vaitiolovelvollisuutta tulee noudattaa myös työsuhteen päätyttyä. Euroopan parlamentin ja neuvoston asetuksessa (EU) 2016/679 on määritelty, että henkilötietorekisterin pitäjän tulee pystyä osoittamaan, että henkilötietojen käsittelytoiminnassa on noudatettu tietosuojavaatimuksia ja käytetty tarvittavia teknisiä, hallinnollisia ja organisaatiollisia toimenpiteitä. Tietosuojalakia noudatetaan rinnakkain tietosuoja-asetusten kanssa. Laissa käsitellään tarkemmin henkilötietojen käsittelyn oikeusperusteista. Tietosuojalaki on korvannut henkilötietolain (523/1999).

Tietosuoja-asetuksessa määritellään, että henkilöillä on oikeus tulla unohdetuksi. Tämä käytännössä tarkoittaa, että yksityiset henkilöt saavat päättää, ovatko heidän henkilötietonsa tietokannoissa. Tällöin yksityisillä henkilöillä on oikeus saada tietää, mitä tietoja heistä on ja pitääkö kyseiset tiedot poistaa heidän pyynnöstään. Tähän lakiin on kuitenkin poikkeus: tietokannassa rekisterinpitäjällä on lain velvoite säilyttää tiedot rekisterissä, ei niitä yksityishenkilön pyynnöstä poisteta [10].

Kirkon yleisissä tietoturvamääräyksissä määritellään, että jäsentietojärjestelmän eli kirjurin käyttäminen KIRKKO-verkon ulkopuolelta on kiellettyä [11]. Covid-19-epidemian aikana kuitenkin kirkon säädöskokoelmassa (KS) erikseen määrättiin väliaikainen etätyön mahdollistava poikkeustilanne. Väliaikeisessa määräyksessä mahdollistetaan kirkon jäsentietorekisterin käyttö etänä epidemia aikana. Tällöin kirkon yleisen tietoturvamääräyksen kohtaa 2.1.7 ei sovelleta. [12.]

5.2 Ratkaisuja Kirjurille

Kirjuriin liittyvä laki on hyvin tiukka, ja kyseiset lakipykälät vaikuttavat vahvasti nykyisen KIRKKO-verkon kokonaisuuden toimintaan. Nykyinen KIRKKO-verkko on koottu Kirjurin käytön ympärille, ja nykyiset verkkojärjestelyt ovatkin riippuvaisia Kirjurista. Kirjurin käytön uudistaminen poikkeusolosuhteiden ulkopuolella mahdollistaisi huomattavasti laajemmat mahdollisuudet KIRKKO-verkon kehitykseen tulevaisuudessa.

Kirjurin perusratkaisut eivät ole muuttuneet juurikaan, sen jälkeen, kun kyseinen järjestelmä on otettu käyttöön. Nykyinen kirjautumiseen liittyvä järjestely on ollut käytössä Kirjurin alusta saakka. Tällä hetkellä käytössä olevat varmennekortit ovat vanhaa teknologiaa ja hyvin epäkäytännöllisiä uusien tunnistautumistapoihin verrattuna. Vanhat tunnistautumiskortit voitaisiin ottaa kokonaan pois käytöstä ja korvata ne uudemmilla kaksivaiheisilla tunnistautumistavoilla. Uudeksi tunnistautumistavaksi kannattaa ottaa puhelintunnistautuminen. Uudessa tunnistautumistavassa kirjautumisen tunnistautuminen tehtäisiin puhelimen kautta. Kirjautuessa Kirjuriin tarvittaisiin jatkossa oma z-tunnus ja puhelin, joka on yhdistettynä uuteen varmennejärjestelmään. Tällöin vanhat varmennekortit voitaisiin ottaa pois käytöstä ja niiden sijaan käyttää joko työpaikan puhelinta tai henkilökohtaista puhelinta tunnistautumiseen. Uusi tunnistautumistapa olisi helpompi ylläpitää ja monipuolisempi. Kirjuria käyttävät työntekijät voidaan laitehallinnassa laittaa Kirjurin käyttäjälistaan, jolloin heillä on oikeus kirjautua Kirjuriin ja varmenteet toimivat heidän kohdallaan. Vastaavasti käyttäjät voidaan poistaa listalta työsuhteen päätyttyä. Uuden varmennetavan käyttöönotossa pitää työntekijöiden antaa tarvittavat tiedot, kuten puhelinnumerot (työ- ja henkilökohtainen) ja sähköpostiosoite, jotta laitteiden rikkoutuessa tai kadottaessa, vanha laite voidaan deaktivoida ja uudet laitteet voidaan helpommin ottaa käyttöön.

KIRKKO-verkon uudistusprojektissa Kirjuriin liittyviä ongelmia on kuitenkin useita. Jos Kirjuriin liittyvät lakipykälät ovat jatkossa yhtä tiukat kuin nyt, on tulevaisuudessa pakko jatkaa KIRKKO-verkon kehitystä Kirjuriin riippuvaisena. Ennen Covid-19-epidemiaa Kirjuria ei ole aikaisemmin saanut käyttää etänä ollenkaan. Haasteena onkin luoda Kirjurin etäkäyttöä varten ympäristö, joka noudattaa nykyistä lainsäädäntöä. Tulevaisuudessakin tullaan tarvitsemaan KIRKKO-verkkoa, koska tiukka lainsäädäntö yksityisyyden suojasta ei ole lievenemässä.

6 Tietoturva ja fyysinen turva

Verkon liittymien tietoturvaa ylläpitää IT-alueen isäntäseurakuntataloudet, sillä tietoturvaa koskevat säännökset ovat yleisiä ja koskevat täten kaikkia IT-alueita

ja seurakuntia. Jokaisella IT-alueella kuuluu olla oma tietoturvavastaava, jonka tehtäviin tulee seurata ja varmistaa, että tietoturva-asetuksia ja lakeja noudatetaan IT-alueen sisällä. Seurakunnat saavat kuitenkin vaikuttaa omiin tietoturvapäätöksiinsä, kunhan tietoturvaan liittyviä yhteisiä säädöksiä ja lakeja noudatetaan. Yhteiset tietoturvasäädökset ovat kirkonhallintorakenteen toteutuksen takia hyvin yleisluontoisia ja tulkittavissa usealla eri tavalla, joten IT-alueiden tietoturvaa on saatettu toteuttaa usealla eri tavalla. Vaikka tietoturvamääräykset ovat jokseenkin tulkittavissa, on niiden yleinen tietoturvataso korkea. Kun on kyse Kirjuriin liittyvistä tietoturvamääräyksistä ne ovat tiukat ja noudattavat Suomen valtion säätämiä tietoturvaan liittyviä määräyksiä.

Kirkon yleisissä tietoturvamääräyksissä määritellään, että ulkopuolisilta toimijoilta vaaditaan sama tietoturvataso kuin kirkon omassa toiminnassa. Ulkopuolisten urakoitsijoiden siis tulee noudattaa samoja tietoturvamääräyksiä ja salassapitosopimuksia kuin kirkon oman henkilöstön. Tietoturvavaatimukset uusille yhteistyökumppaneille asetetaan jo tarjouspyyntö- tai sopimusneuvotteluvaiheessa. [13.]

IT-alueet eivät tarjoa suoranaisesti fyysiseen turvaan liittyviä palveluita, kuten videovalvontaa tai vartijoita. Seurakunnat saavat itse päättää, mihin haluavat videovalvonnan sijoittaa ja tarvitseeko rakennukset tai muut tilat vartiointia. IT-alueet saattavat kuitenkin tarjota videokuvatallenteille tallennuspaikan omasta konehuoneestaan. IT-alueen asiantuntijat voivat myös tarjota konsultaatioita fyysisen turvan toteuttamiseen, mutta useissa tapauksissa seurakunnat hoitavat omat valvontaan ja fyysiseen turvallisuuteen liittyvät tehtävät.

Pilvipalveluihin liittyvää tietoturvaa tulee tarkastella tulevaisuudessa nykyistä enemmän. Vielä toistaiseksi, kun pilvipalveluita ei ole otettu kokonaisvaltaisesti kaikkialla käyttöön, ovat tietoturvariskit alemmat kuin ne tulevaisuudessa tulevat olemaan. Tulevaisuudessa luultavasti päädytään luopumaan omista konesaleista ja palvelimista IT-alueilla. Täten kannattaa jo nyt alustavasti tarkastella varmuuskopiointi, turvatulostus ja salassa pidettävän materiaalin pilvipalvelu- ja tietoturvaratkaisuja. Pilvipalveluita hyödyntäessä kannattaa tietoturvan kannalta

hankkia palvelimet EU-alueelta, jotta GDPR (General Data Protection Regulation) on voimassa. GDPR on henkilötietojen käsittelyä koskeva yhteinen EU-maiden tietosuoja-asetus. [14.] On kuitenkin huomioita, että palvelimiin liittyvässä lainsäädännössä noudatetaan sen maan lainsäädäntöä, jossa palvelimet sijaitsevat.

6.1 Fyysisten laitteiden tietoturva

Monitoimilaitteet, kuten tulostimet, toimivat käyttäjätunnuksen tai korttitunnistuksen avulla. Turvatulostuksessa tulostettava materiaali latautuu turvatulostuspalvelimelle, jolloin tulostettava materiaali pystytään tulostamaan laitteilta, jotka ovat yhteydessä turvatulostuspalvelimeen, jos tarvittava tunnistautuminen tulostuksen yhteydessä toteutuu. Turvatulostuksessa on tärkeää, että monitoimilaite ja turvatulostuspalvelin pystyvät kommunikoimaan keskenään, jotta turvatulostus on mahdollista. Monitoimilaitteiden toiminta tulee ottaa huomioon, jos MFA-tunnistautuminen otetaan käyttöön, koska MFA-muutos tarkoittaisi tunnistuskorttien käytöstä poistamista. Tällöin tulostuslaitteisto voisi jatkossa vaatia vain käyttäjätunnuksen. Vaihtoehtoisesti jos tiukemmalle tietoturvalle nähdään tarve, voidaan MFA-tunnistautumisvaihtoehtoja tarkistella tulevaisuudessa myös monitoimilaitteistolle.

Videovalvontaa toteutetaan IT-alueilla hyvin samalla tavalla. IT-alueita vetävä seurakuntatalous ei päätä IT-alueen sisäisten seurakuntien kameravalvonnasta. Seurakunnat saavat itse päättää, mihin valvontaa laitetaan ja mihin valvontavideomateriaali tallennetaan. Yleisimmin seurakuntayhtymä hoitaa kiinteistöjen videovalvonnan alueellaan.

Tallennustapoja on erilaisia. Esimerkiksi videotallenteiden lataaminen seurakunnan tai IT-alueen servereille on myös mahdollista, että tallennustila ostetaan pilvipalveluna joltain ulkoiselta yritykseltä. Täten tallenteet ja varmuuskopiot videokuvasta menevät yrityksen x palvelimille. Suositeltavaa olisi siirtyä palveluntarjoajien palvelimiin.

6.2 Tietoturvan implementointi

Olisi suositeltavaa, että hyödynnettäisiin pilvipalveluita videomateriaalin tallentamiseen, koska omista palvelinsaleista ollaan hiljalleen luopumassa. Pilvipalveluiden hyödyntäminen videokuvan tallentamiseen saattaa olla osittain hankalaa, sillä videotallenteet vievät paljon tallennustilaa, mikä vaikuttaa suoranaisesti kustannuksiin. Tallennustilaan liittyviä kustannuksia voitaisiin vähentää videokuvamateriaalin automaattisella poistamisella tallennusserveriltä esimerkiksi 14 vuorokauden kuluessa, ellei kyseistä videokuvamateriaalia tallennetta manuaalisesti pidempiaikaiseen tallennustilaan. Mikäli järjestelmä uudistetaan, henkilöstö, joilla on oikeus valvontakuvamateriaalin tarkasteluun, tulee kouluttaa uuteen järjestelmään. IT-alueiden omien palvelimen käyttö voi toistaiseksi olla hyvä tapa hoitaa videomateriaalin tallennus, mutta haastatteluissa kävi ilmi, että suuri osa IT-alueista on vähentänyt tai ovat vähentämässä omia palvelimia, koska ulkoiset palveluiden tarjoajat pystyvät nykyisyydessään tarjoamaan edullisempia hinnastoja palveluilleen. Tämä tarkoittaa, että tulevaisuudessa IT-alueen palvelimet eivät enää ole käytössä, ja täten pilvitallennus on tulevaisuuden ratkaisu. Toistaiseksi kuitenkin IT-alueiden palvelimien käyttö joissain tapauksissa saattaa olla edullisempaa kuin ulkoiset pilvipalvelut. Tallennusten siirtäminen IT-alueilta ulkoisille palveluntarjoajille ei ole toistaiseksi kiireellistä.

Tallennustilaan liittyvät vaikeudet eivät kuitenkaan ole ainoa ongelma, sillä videomateriaalin käsittelyyn liittyen on standardeja, joiden mukaan vain tietty henkilöstö saa katsella kuvamateriaalia. Pilvipalvelualustojen hyödyntämistä valvontakameratallennuksiin kannattaa konsultoida nykyisiä tietoturvavastaavia ja käyttöoikeushallinnasta vastaavia henkilöitä (niin sanotut ”pääkäyttäjät”), jotta pilvipalveluihin ladattavaa materiaalia pystyttäisiin mahdollisimman tietoturvallisesti ja vastuullisesti käsittelemään.

Pilvipalveluiden fyysiseen sijaintiin ja tietoturvaan liittyvät implementoinnit ovat tulevaisuudessa isossa roolissa kirkon IT-rakenteen uudistuksessa. Kannattavaa olisi joko perustaa oma koko kirkon yhteinen palvelin tai ostaa pilvipalvelu

Suomen rajojen sisällä toimivalta yritykseltä, joka kuuluu huoltovarmuusorganisaatioon. Tulevaisuudessa kaikki IT-alueet voisivat varmuuskopioida kaiken kirkon toiminnan kannalta oleellisen materiaalin kyseisille palvelimille, jolloin kriisitilanteessa salassa pidettävät tiedot ja kirkon toiminallisuuden mahdollistava materiaali on turvassa ja käytettävissä riippumatta ulkomaisista tahoista. Oman palvelinhallin rakentaminen on huomattavasti kalliimpaa, eikä tätä ratkaisua kannata tehdä, jos vain on mahdollista saada pilvipalvelut tilattua kolmannen osapuolen toimittajalta. Oman palvelimien kustannukset nousisivat huomattavasti yli valmiina olevan palveluntarjoajan kustannustason, koska oman konesalin ylläpitokustannuksien lisäksi pitää ottaa huomioon laitehankinnat, paikka, mihin palvelimet laitettaisiin ja osaavien työntekijöiden palkkaaminen huoltoja ja käyttöä varten. Tilanteessa, jossa olisi mahdotonta löytää sopivaa toimittajaa pilvipalveluiden toiminnan varmistamiseen kriisitilanteen aikana tai sen jälkeen on kuitenkin hyvä tehdä katsaus mahdollisiin omiin palvelimiin.

KIRKKO-verkon uudistusprojektin myötä suunniteltu 4G-verkon käyttöönotto ei estäisi fyysiseen turvaan liittyviä uudistuksia. 4G-yhteydet voisivat päinvastoin avustaa paikallisten ratkaisuiden uudistamista pilvipalveluihin. 4G-verkko kykenee siirtämään videokuvaa ja tiedostoja riittävällä nopeudella uusille palvelinalustoille.

7 Ongelmat ja riskit

IT-alueiden haastatteluissa kävi ilmi, että IT-alueiden välillä ei ole riittävästi yhteistyötä ja kommunikaatiota tulevaisuuden suunnitelmista. Ajatuksia uudistuksiin liittyvissä asioissa ei välttämättä kerrota muille. IT-alueet ovatkin hyvin varovaisia, sillä uudistuksien pelätään vaikuttavan vakavasti IT-alueiden tarpeellisuuteen ja täten suoranaisesti työllisyyteen. Kyseisistä syistä IT-alueet saattavat reagoida negatiivisesti uudistushankkeessa. Työpaikkojen väheneminen kirkon IT-alalta ei ole todennäköistä, mutta työtehtävien perustehtävä on jatkuvassa muutoksessa. Tämä aiheuttaa haasteita mm. uudelleenkouluttamiselle. Teknologian edistyessä tarvitaan vähemmän työntekijöitä hallitsemaan suuria

kokonaisuuksia. Silti ylläpitotehtävät tarvitsevat näköpiirissä olevassa tulevaisuudessa nykyisen määrän IT-ammattilaisia. Toisaalta IT-alan osaajien määrää kirkossa ei tarvitse myöskään kasvattaa.

Ongelmiin voidaan lisätä myös erilaiset näkemykset IT-alueiden välillä uudistuksiin liittyen. Osa IT-alueista on tyytyväisiä nykyiseen järjestelmään eikä näe syytä ottaa uusia uudistusehdotuksia huomioon. Vastaavasti myös koetaan, etteivät uudet ehdotukset välttämättä pysty hoitamaan uudistettavaa kohdetta yhtä hyvin kuin nykyisellä tavalla asia hoidetaan. Esimerkkinä tästä on IT-tukeen liittyvä uudistus, jossa IT-tukipyyntöjä jaettaisiin kaikille IT-alueille nopeamman ratkaisun saamiseksi IT-ongelmiin. Todellisuudessa IT-tukeen liittyvässä uudistuksessa olisi useita ongelmia eri järjestelmien välillä, joten uudistusta ei ole toistaiseksi tehty. Uudistuksissa voi myös tulla paikallisen IT-alueen palvelutasoa heikentäviä elementtejä, joiden takia alueet eivät välttämättä halua uudistusta tehdä. Uudistusehdotukset saattavat myös sisältää muutosesityksiä, joissa ei ole otettu huomioon muiden IT-alueiden tarpeita. IT-alueet kattavat koko Suomen. On paikkoja, joihin tietynlaiset ratkaisut ovat mahdottomia tai saattaisivat luoda liian suuria kuluja yksittäisten IT-alueiden kustannettavaksi.

Riskien tiedostaminen ja selvittäminen on osa kaikkia projekteja. Riskien ymmärtäminen ja tiedostaminen huomattavasti helpottaa erilaisten projektien toteuttamista, koska riskeihin varautuminen nopeuttaa projektin toteutumista ongelman ilmetessä. Riskien tarkastelu auttaa myös projektissa osallisena olevia työntekijöitä ymmärtämään, kuinka mahdolliset ongelmatilanteet tulisi ratkaista.

Suurimpiin riskeihin kuuluu uudistuksen implementoinnin yhteydessä tulevat käyttökatkokset, yhteensopivuusongelmat ja mahdollinen kulujen nousu. Suurien tietoverkkouudistuksien aikana on aina riski, etteivät ohjelmistot tai yhteydet toimi kuten on alun perin odotettu. Nämä käyttökatkokset saattavat tuottaa suuria ongelmia, koska työntekijät eivät välttämättä pysty hetkellisesti hoitamaan omia työtehtäviään. Käyttökatkokset voivat johtua useasta eri asiasta, mutta usein kyseessä on konfiguraatiopäällekkäisyydet tai virheet verkkolaitteistossa tai laitteiston yhteensopivuusongelmat isossa kokonaisuudessa. Konfiguraatio-

ongelmat voivat ilmetä päällekkäisyyksinä reitityksissä. Koska IT-alueet saavat hoitaa kaiken omaan toimintaansa liittyvät asiat, ei yhteisiä standardeja laite- ja ohjelmistohankinnoissa ole. Tämä tuottaa suuria yhteensopivuusongelmia, jos nykyistä KIRKKO-verkkoa lähdettäisiin radikaalisti muuttamaan.

Yhtenä riskinä on kulujen nousu. Oletettavasti kulut nousevat vain hetkellisesti uudistuksen alussa, mutta erilaiset sopimukset eri IT-alueilla saattavat nostaa yksittäisten IT-alueiden kokonaiskuluja pidemmällä aikavälillä. Riski kulujen nousuun muodostuu, kun eri IT-alueet toteuttavat verkkoratkaisunsa hyvin erilaisilla tavoilla. Huomioitavaa on kuitenkin, että pienemillä paikkakunnilla saattaa olla kuuluvuuteen liittyviä ongelmia, jolloin verkkoratkaisut on mukautettu paikkakunnan yksittäisiin tarpeisiin.

Riskeissä on myös otettava huomioon globaalit tekijät kuten eri maiden poliittiset muutokset tai taloustilanteet. Erilaisten palveluiden hankinta ulkomailta saattaa olla edullisempaa ja tarjonta parempaa. Mahdollista on kuitenkin, että palvelut saattavat hetkellisesti katketa ulkoisen tekijän toimesta.

Pilvipalveluoperaattorien sopimukset saattavat myös luoda suuren kuluriskin. Pilvipalveluoperaattorit saattavat piilottaa suuret kulut datansiirtoon pois omilta palvelimiltaan. Uuden palvelun käyttöönottaminen saattaa olla kuitenkin halpaa.

Riskien hallinnalla on suuri merkitys kaikissa uudistusprojekteissa. Yleisesti ottaen riskienhallinta on osa jokaista projektia. Kaikissa projekteissa tulee tiedostaa, mitä riskejä projekti sisältää ja miten kyseisiä riskejä voidaan minimoida ja hallita.

Projektiin sisältyvät riskit on mainittu edellisessä osiossa. Näitä kyseisiä riskejä voidaan minimoida hyvällä suunnittelulla ennen projektin varsinaista toteutusta. KIRKKO-verkon uudistuksessa on tarkoituksena modernisoida KIRKKO-verkon infrastruktuuri. KIRKKO-verkon muutoksen aikana kannattaa täten suunnitella suurimpien muutosten tekemistä kiireisimpien työtuntien ulkopuolella. Suurim-

mat muutokset, kuten verkkolaitteiden käytöstä poisto tai konfiguraatiomuutokset, olisi hyvä tehdä normaalien (8-16) työtuntien ulkopuolella. Täten minimoidaan riskit, jotka vaikuttavat suoraan verkkoyhteyksiin eikä mahdollisten käyttökatkoksien aikana IT-tukeen tulisi ruuhkaa. Verkon uudistuksen aikana kannattaakin olla vaihtoehtoinen (esimerkiksi vanha KIRKKO-verkko) yhteys käytettävissä, jotta uudistus ei vaikuta ainakaan huomattavasti kirkon työntekijöiden normaaliin työhön.

Riskienhallintaa KIRKKO-verkon uudistusprojektissa voidaan soveltaa vastaavissa isojen organisaatioiden verkkouudistuksissa.

8 Toimintaehdotus

KIRKKO-verkon uudistus kannattaa aloittaa langattoman verkon kuuluvuuskartoituksella. Langattoman verkon kuuluvuuskartoitusta voidaan tehdä IT-alueittain ja täten nähdään, mihin toimipisteisiin saataisiin alustavasti toimiva langaton verkkoratkaisu. Kuuluvuuksia voidaan myös kysyä operaattoreilta, jolloin saadaan alustava kuva siitä, kuinka kattava langattoman verkon pitäisi paikkakohtaisesti olla. Kuuluvuuskartoituksen jälkeen voidaan aloittaa implementointikokeilut, joiden päämääränä on saada realistinen kuva langattoman verkon kuuluvuudesta ja kuuluvuuteen liittyvistä ongelmista. Paikoissa, joissa kuuluvuus on hyvä, voidaan asentaa tarvittavat verkkolaitteistot paikalleen ja ottaa langaton verkko käyttöön. Heikoilla kuuluvuusalueilla voidaan tehdä paikallisia ratkaisuja esimerkiksi ottamalla käyttöön vahvistimia. Jos vahvistimista tulevat kulut ovat liian suuret hyötyyn verrattuna tai kuuluvuusongelmat eivät ratkea edes vahvistinantennien kanssa, voidaan vielä toistaiseksi vanhat yhteydet jättää käyttöön.

Oletettavasti kaikkialla Suomessa langaton verkko ei toimi toivotulla tavalla, joten useampia eri liitäntätapoja tulee jäämään käyttöön. Usean eri liitäntätavan verkossa olisi suositeltavaa ottaa käyttöön SD-WAN-verkkoratkaisu, jolloin verkon hallinta uudistuksen aikana olisi mahdollisimman helppoa. SD-WAN-palvelun implementointiin liittyvissä kysymyksissä kannattaa olla yhteydessä kyseisen palvelun tarjoajiin.

Langattoman verkon käyttöönotossa voi ilmetä ongelmia Kirjurin käyttöön liittyvissä lakiasioissa. Kirjurin käytössä saattaa ilmetä hankaluuksia langattomien internetyhteyksien kanssa, koska nykyisessä laissa on tarkat vaatimukset kirjurin käyttöön liittyen. Laki tulisi muuttaa siten, että se mahdollistaa Kirjurin käytön langattomassa verkossa. Laki muutosehdotuksessa kannattaa huomioida, kuinka uudistuslainsäädäntö vaikuttaisi laitehallintaan ja käyttäjien tarpeisiin kuten helppokäyttöisyys. Lakimuutokseen liittyen voi tehdä myös uudistuksen varmennukseen. Varmennekortit voidaan ottaa pois käytöstä ja siirtää varmennus pilvipalveluun. Monivaiheinentunnistus puhelimien kautta mahdollistaisi Kirjurin käyttöoikeuksien nopeamman aktivoimisen ja mahdollisissa laitteiden katoamistai rikkoutumistapauksissa laitteet voidaan nopeasti deaktivoida. Alustavasti kannattaa pyrkiä muuttamaan kaikki langattomaksi ja jättää vain Kirjuri KIRKKO-verkkoon.

Pilvipalveluiden käyttöä voidaan lisätä tulevaisuudessa verkkouudistuksen mukana. Tällä hetkellä melkein kaikilla IT-alueilla on omat palvelimensa, mutta halukkuus päästä omista palvelimista on yleinen suunta kaikilla alueilla. Pilvipalvelut kannattaisi yhtenäistää hankkimalla samat ohjelmistot yhteisesti samalta palveluntarjoajalta. Tulevaisuudessa yhtenäiset linjaukset pilvipalveluiden käytössä helpottaisivat hallintaprosessia ja tehostaisivat työtä kaikkialla kirkossa. Pilvipalveluiden hallinta oikeudet tulevat olemaan jännitteinä ja niiden ratkaiseminen uudistuksissa olisikin tärkeää. Mahdollisiin ratkaisuihin voidaan ajatella omia tenantteja eri IT-alueilla, mutta kyseinen ratkaisu olisi väliaikainen, koska todellisuudessa omat yksittäiset tenantit ovat tarpeettomia menoeriä, jotka luultavasti tullaan karsimaan tulevaisuudessa pois. Muutoksen ei tarvitse tapahtua samanaikaisesti verkko uudistuksen kanssa, mutta yhteisestä suuresta IT-infrastruktuurimuutoksesta voitaisiin alkaa laatia suunnitelmaa yhteistyönä kaikkien IT-alueiden välillä. Ymmärrettävää on, ettei jokainen IT-alue halua muutosta, mutta yhteisen toimintasuunnitelman alustava muotoilu ei tulisi rikkomaan nykyistä toimintamallia.

Yhteistyön lisääminen IT-alueiden välillä olisi suositeltavaa. Yhteistyötä voidaan lisätä tekemällä yhteisiä toimintasuunnitelmia. Toimintasuunnitelmat voivat olla

alustavia kaikkien IT-alueiden välillä. Kannattavaa olisi tehdä IT-alueiden välillä sopimuksia, jotka mahdollistavat IT-alueiden toiminnan myös poikkeusolosuhteissa. Esimerkkinä voidaan antaa IT-alueiden väliset IT-tukisopimukset, jotka mahdollistaisivat IT-tuen toiminnan, vaikka yksi IT-alue lamaantuisi väliaikaisesti. IT-alueet voisivat tehdä yhden tai useamman IT-alueen kanssa sopimuksen IT-tuen hoitamisesta poikkeusolosuhteissa, joka tarkoittaisi tutustumista toisten IT-alueiden toimintaan. Tarkoituksena ei ole kuitenkaan omaksua täysin toisten IT-alueiden toimintamallia, mutta mahdollisia parannuksia omaan IT-aluetoimintaan voidaan huomata tekemällä enemmän yhteisteistyötä IT-alueiden välillä. Kirkon sisälle voitaisiin perustaa toimielin, jonka tehtävänä olisi tulevaisuudessa tehdä toimintasuunnitelmia ja varmistaa, että toimintasuunnitelmat toteutuvat halutulla tavalla. Kyseisen toimielimen jäsenet voitaisiin koota eri IT-alueilta, jotta kaikkien ajatukset uudistuksiin liittyen saadaan esille. Yhtenä yhteistyön tavoitteista olisi luoda IT-asioiden neuvottelukunta, jonka tehtävänä on valmistella yhteiset linjaukset IT-uudistuksiin kirkkohallinon täysistunnon päätettäväksi.

Suuren Infrastruktuurin muutoksen yhteydessä kannattaisi tehdä toimintasuunnitelma jatkokoulutuksista IT-ammattilaisten siirtämiseksi uusiin tehtäviin riskeeraamatta työpaikkoja. Jatkokoulutukset tulisi aloittaa mahdollisimman nopeasti, jotta siirtyminen uusien teknologioiden käyttöön olisi sulavaa.

9 Yhteenveto

Tilaustyönä tehty KIRKKO-verkon uudistusprojekti on selvitystyö, jonka tavoitteena on tehdä ehdotus Suomen evankelisluterilaiselle kirkolle, kuinka kirkon IT-infrastruktuuria tulisi uudistaa. Projektin osa-alueina ovat KIRKKO-verkko ja siihen liittyvät liitännät ja sopimukset, pilvipalvelut, ohjelmistot, laitehallinta sekä IT-tuki. Työssä käsitellään myös kirkon hallinnollista rakennetta ja lakiasioita, jotka vaikuttavat uudistusehdotukseen.

Työ aloitettiin kartoittamalla KIRKKO-verkko liitännöiden määrä ja niiden nopeudet sekä operaattorisopimukset ja verkkolaitteisto. Kartoitus tehtiin haastatteluilla. Haastateltavina olivat kirkon IT-alueiden tietohallintopäälliköt ja IT-asiantuntijoita. Haastateltavien pyynnöistä johtuen projekti ei sisällä suoria lainauksia haastatteluista. Haastattelut kuitenkin antavat kokonaiskuvan KIRKKO-verkon laajuudesta ja siihen liittyvistä uudistustarpeista.

KIRKKO-verkon uudistusehdotuksessa suositellaan kiinteiden liittymien käytöstä poistamista ja siirtämistä KIRKKO-verkko kokonaan langattomaan 4G-verkkoon. Työssä on kuitenkin huomioitu maantieteelliset sijainnit, joihin langattomia verkkoyhteyksiä ei välttämättä pystytä toteuttamaan. Tämän takia työssä suositellaankin ottamaan käyttöön SD-WAN-verkkoarkkitehtuuriratkaisu, jolloin jäljelle jääviä kiinteitä yhteyksiä voidaan hallita helposti langattomien yhteyksien rinnalla.

Yhteisen toimintasuunnitelman tekeminen IT-alueiden välillä olisi tärkeää, jotta tulevaisuuden toteutuksissa kaikki IT-alueet olisivat liikkumassa samaan suuntaan ja täten yhteistyö helpottuisi kirkon sisällä. Yhteisten linjausten tekeminen mahdollistaisi kokonaisuuksien helpomman hallinnan ja täten laskisi kuluja.

KIRKKO-verkon uudistus vaatisi kuitenkin joitakin lakimuutoksia, jotka mahdollistaisivat jäsentietojärjestelmä Kirjurin tietoturvallisen etäkäytön ja muutoksen, joka antaisi kirkkohallituksen täysistunnolle oikeuden päättää kaikista keskeisistä Suomen Evankelisluterilaisen kirkon tulevaisuuden IT-uudistuksista. Valmistelua varten kirkkohallitus voi perustaa IT-asioiden neuvottelukunnan.

Lähteet

1. KIRKKO-verkon pääsopimus, liite 1.1 KIRKKO-verkon palvelukuvaus sivu 1. (Salainen) Luettu 08.12.2020.

2. Sopimus KIRKKO-verkon tietoliikennepalveluista, liite 1.1 KIRKKO-verkon ydin sivu 1. (Salainen) Luettu 14.12.2020.

3. Kirkon organisaatio. Verkkoaineisto. Suomen Evankelisluterilainen kirkko <https://evl.fi/tietoa-kirkosta/kirkon-organisaatio>. Luettu 16.12.2020.

4. Mitä SD-WAN tarkoittaa ja kenelle se sopii? 2019. Verkkoaineisto. DNA Oyj. <https://www.dna.fi/yrityksille/blogi/-/blogs/mita-sd-wan-tarkoittaa-ja-kenelle-se-sopii>. Päivitetty 13.5.2019 Luettu 01.03.2021.

5. air gapping (air gap attack). 2017. Verkkoaineisto. TECHTARGET. <https://whatis.techtarget.com/definition/air-gapping>. Päivitetty syyskuussa 2017. Luettu 04.03.2021.

6. Microsoft Intune is an MDM and MAM provider for your devices. 2020. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune>. Päivitetty 23.06.2020. Luettu 04.01.2021.

7. KJ Dearie. 2020. What is EULA? Verkkoaineisto. Termly. <https://termly.io/resources/articles/what-is-eula/>. Päivitetty 16.11.2020. Luettu 15.12.2020.

8. Laura Vainio. 2019. Yrittäjä: Tunnetko nämä tietoturvan termit? Verkkoaineisto. Telia <https://www.telia.fi/yrityksille/artikkelit/artikkeli/tietoturva-sanasto-yrittajille>. Päivitetty 01.08.2019. Luettu 21.01.2021.

9. What is Azure ExpressRoute? 2020. Verkkoaineisto. Microsoft. <https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction>. Päivitetty 05.10.2020. Luettu 11.02.2021.

10. Virastonhoidon ohjeet, Henkilötietojen käsittely. (Salainen) Luettu 04.01.2021.

11. Kirkon yleiset tietoturvamääräykset. 2019. Verkkoaineisto. Suomen evankelisluterilainen kirkko.
Kirkon yleiset tietoturvamääräykset sivu 9 kohta 2.1.7.
<https://evl.fi/documents/1327140/43075208/Kirkon+yleiset+tietoturvam%C3%A4%C3%A4r%C3%A4ykset+1.1.2020.pdf/0c0c16b3-e399-d83b-19d9-50fb735323d1?t=1576581174000>
Päivitetty. 21.3.2019. Luettu 20.01.2021.

12. Kirkon säädöskokoelma Nro 143 Kirkkohallituksen väliaikainen määräys tietoturvapolitiikasta. 2020. Verkkoaineisto. Suomen evankelisluterilainen kirkko.
<https://evl.fi/documents/1327140/60545655/31_2020+liite+143-2020_Kirkkohallituksen+v%C3%A4liaikainen+m%C3%A4%C3%A4r%C3%A4ys+tietoturvapolitiikasta.pdf/38a8d4df-f46c-9856-e7f7-116ca1c03505?t=1609760479759>.
Päivitetty 15.12.2020. Luettu 03.02.2021.

13. Kirkon yleiset tietoturvamääräykset. 2019. Verkkoaineisto. Suomen evankelisluterilainen kirkko.
Kirkon yleiset tietoturvamääräykset sivu 6 kohta 1.3.
<https://evl.fi/documents/1327140/43075208/Kirkon+yleiset+tietoturvam%C3%A4%C3%A4r%C3%A4ykset+1.1.2020.pdf/0c0c16b3-e399-d83b-19d9-50fb735323d1?t=1576581174000>.
Päivitetty 21.3.2019. Luettu 20.01.2021.

14. Usein kysyttyä EU:n tietosuoja asetuksesta. 2018. Tietosuojavaltuutetun toimisto.
<https://tietosuoja.fi/gdpr>.
Luettu 25.02.2021.

Haastatellut

Haastateltavien toivomuksesta viitteitä haastatteluihin ei ole nootitettu.

Björn Mika Järjestelmäasiantuntija (Oulun seurakuntayhtymä)

Heickell Sanna Rekisterijohtaja (seurakuntarekisterit)

Herrala Aki Johtava IT-asiantuntija (Ylivieskan seurakunta)

Kettunen Satu Järjestelmäpäällikkö (seurakuntarekisterit)

Koskinen Timo Tietohallintopäällikkö (Turun ja Kaarinan seurakuntayhtymä)

Krapu Antti Palvelupäällikkö (talousosasto)

Kuusivuori Seppo Tietohallintopäällikkö (Hallinto-osasto)

Kähkölä Jari Tietojärjestelmäpäällikkö (talousosasto)

Lahti Jyrki Tietohallintopäällikkö (Kouvolan seurakuntayhtymä)

Lahtinen Jouni Tietohallintopäällikkö (Jyväskylän seurakunta)

Laukkarinen Pekka Tietohallintopäällikkö (Kuopion seurakuntayhtymä)

Mukari Jussi Tietoturvapäällikkö (talousosasto)

Mustonen Kristian Tietohallintopäällikkö (Rovaniemen seurakunta)

Pekkarinen Pentti Tietohallintopäällikkö (Oulun seurakuntayhtymä)

Pulkkinen Keijo ICT-kehityspäällikkö (Tampereen seurakuntayhtymä)

Sahi Kimmo IT-suunnittelija (talousosasto)

Salo Kalervo Kirkkoherra (Espoon seurakuntayhtymä)

Saukkonen Simo Tietohallintopäällikkö (Lahden seurakuntayhtymä)

Sundqvist Erland Tietohallintopäällikkö (Pietarsaaren Seurakuntayhtymä)

Tamminen Jukka Tietohallintojohtaja (talousosasto)

Tevilin Kari Tietohallintopäällikkö (Espoon seurakuntayhtymä)

Liitteet

IT-alue-erittelyt

Luettelo IT-alueista ja niiden sisältämistä teknisistä yksityiskohdista on opinnäytetyön tekijällä tiedossa, mutta tiedot ovat salaisia.