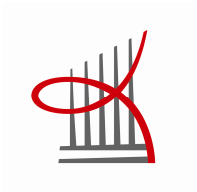


MOBIILILAITTEIDEN ETÄHALLINTA

FROMDISTANCE MDM-TUOTETTA KÄYTTÄEN

Mari Ahonen

Opinnäytetyö
Huhtikuu 2011
Tietotekniikka
Tietoliikennetekniikka
Tampereen ammattikorkeakoulu

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikka
Tietoliikennetekniikka

AHONEN, MARI: Mobiililaitteiden etähallinta FromDistance MDM -tuotetta käyttäen

Opinnäytetyö 38 sivua
Huhtikuu 2011

Tutkintotyön aiheena oli FromDistance MDM -ohjelmisto, jota käytetään mobiililaitteiden etähallintaan.

Työn tarkoituksena on pilotoida kyseistä ohjelmistoa yrityksen käyttöön, ja tarkastella ohjelmiston käyttömahdollisuuksia yrityksen tarpeiden kannalta. Suurimpina tarpeina ovat ennen pilotointia olleet käsin tehtävän työn vähentäminen sekä muissa yrityksen toimipisteissä työskentelevien henkilöiden etätuen mahdollistaminen.

Tässä työssä esitellään FromDistance MDM –ohjelmiston käyttöä ja hallinnointia, kyseisen ohjelmiston turvaominaisuuksia sekä eräitä sähköisen viestinnän tietosuojalakiin sekä henkilön tunnistamis- ja paikkatietojen seurantaan liittyviä lakiteknisiä seikkoja.

Asiasanat: Mobiililaite, etähallinta, laitehallinta

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University Of Applied Sciences
Computer technology training program
Telecommunications and Information Networks

AHONEN, MARI: Remote management on mobile devices using the FromDistance MDM product

Bachelor's thesis 38 pages
April 2011

This thesis is a study of a remote mobile management solution, FromDistance MDM.

The purpose of this thesis is to pilot the solution for company use and to evaluate the opportunities of the solution from the point of view of the company's needs. The biggest need so far has been to minimize the manual work on installing software on the phones and to offer remote support to employees working in distant offices.

The thesis will introduce the using and administrating the FromDistance MDM solution, the security features of it and some of the legal facts in the Finnish Privacy Protection Act.

Keywords: Mobile device, remote management, device management

Esipuhe

Tämä työ ja siihen liittyvä tutkimustyö on tehty vuosien 2009-2011 välillä. Tutkimustyöhön sisältyy Insta Group Oy:n tytäryhtiön Insta DefSec Oy:n työntekijänä tekemäni mobiililaitteiden hallinta, ohjelmistojen kehityksen seuraaminen sekä erilaisiin hallinnointiratkaisuihin tutustuminen. Itse FromDistance MDM –päätelaitehallintaratkaisun pilotointi aloitettiin joulukuussa 2010, ja olen ollut pilotoinnissa mukana alusta alkaen.

Työskentelen Insta DefSec Oy:n alla toimivassa ICT-palveluissa, jonka toimintatavat perustuvat ITIL-prosessikehykseen, ja ovat ISO/IEC 27001-sertifioituja. Näitä prosesseja seuraten yrityksessä hoidetaan myös matkapuhelinhallintaan liittyvät asiat.

Työn tavoitteena oli arvioida MDM-ratkaisun soveltuvuutta yrityksen käyttöön, ja lopulta käyttöönottaa kyseinen järjestelmä. Arviointi on suoritettu tässä opinnäytetyössä. Ohjelmiston hankinnasta ja lopullisesta käyttöönotosta päätetään yhtiötasolla opinnäytetyön tulosten esittelyn jälkeen.

Haluaisin kiittää kaikkia opinnäytetyöprosessissa mukana olleita kollegoitani, erityisesti Heidi Lahtista, joka teki myös oman lopputyönsä tähän aiheeseen liittyen, ja oli kanssani mukana testaamassa ohjelmistoasennuksia. Haluaisin kiittää myös Ari Rantalaa sekä Mauri Inhaa siitä, että vihdoinkin valmistun. Suurimmat kiitokset ansaitsevat kuitenkin avopuolisoni Petri sekä rakkaat kissamme Ninja ja Darwin, jotka kaikki osaltaan auttoivat minua jaksamaan.

Tampereella huhtikuussa 2011

Mari Ahonen

SISÄLLYS

KÄYTETYT LYHENTEET

MDM	Mobile Device Management, Mobiililaitehallinta
OMA	Open Mobile Alliance, Mobiililaitteiden avoin standardikokoelma
OMA-DM	Open Mobile Alliance Device Management
TARM	Terminal Access Rights Management, Etäkäyttöoikeuksien hallinta
VNC	Virtual Network Computing, Etäkäyttötekniikka
VPN	Virtual Private Network, Virtuaaliverkko
SSH	Secure Shell, Tietoliikenteen salausprotokolla
RFB	Remote Framebuffer, Etäkäyttöprotokolla
RSA	Epäsymmetrinen julkisen avaimen salausalgoritmi
TCP	Transmission Control Protocol, verkkoprotokolla
HTTP	Hypertext Transfer Protocol, verkkoprotokolla

1 JOHDANTO

Viime vuosina etätyöskentely ja etäyhteyksien käyttö on yleistynyt huomattavasti työn teossa ja sen joustavuuden lisäämisessä. Etätyön lisääntyminen on johtanut siihen, että töitä tehdään nyt huomattavasti enemmän mobiililaitteilla kuin koskaan aikaisemmin. Mobiililaitteiden käytön lisääminen on taas puolestaan johtanut erilaisten hallintaohjelmistojen tarpeeseen. Insta Groupilla on tällä hetkellä (maaliskuu, 2011) hallinnoitavanaan noin 500 matkapuhelinta, joissa kaikissa on erikseen asennettu tietoturvaohjelmisto. Kyseisen ohjelmiston ajantasaisuuden varmistamiseksi ja laitekannan ylläpidon helpottamiseksi, on yrityksen IT-tukea pyydetty selvittämään mahdollisuuksia mobiililaitteiden hallintaohjelmiston hankintaan ja käyttöönottoon.

Mobiililaitteilla tarkoitetaan älypuhelinten lisäksi myös nk. kämmentietokoneita eli tabletteja. Työssä esiteltävä FromDistance MDM -ohjelmisto tukee useita eri mobiililaitteiden ohjelmistoalustoja, joten ohjelmistolla hallittavista laitteista käytetään tässä työssä yleistä termiä *mobiililaite*.

Puolustusteknologiaan painottuvassa yrityksessä laitteiston tietoturva on huomattavan tärkeä seikka laite- ja ohjelmistohankintoja tehtäessä. Työssä tullaan esittelemään sekä yrityksen vakioidussa valikoimassa olevien älypuhelinten että MDM-ohjelmiston tietoturvaominaisuuksia.

Työ on tehty toimeksiantona Insta DefSec Oy:lle, joka on puolustusteknologian ratkaisuja tarjoava ohjelmistoyritys. Yrityksellä on käytössä tietokoneille suunniteltu laitehallintaohjelmisto, jonka positiivisten käyttökokemusten perusteella on osittain tullut tarve pilotoida myös mobiililaitteille tarkoitettua laitehallintaratkaisua.

2 MATKAPUHELIMET YRITYKSESSÄ

Yrityksen älypuhelinvalikoima on tarkasti rajattu tiettyihin malleihin. Vakioinnilla varmistetaan vahva osaaminen laitteiden ylläpidossa ja käytön opastuksessa. Opinnäytetyöprosessin aikana valikoimaan kuului ainoastaan Nokian puhelinmalleja. Kaikissa valikoiman malleissa on käytössä Symbian-pohjainen käyttöjärjestelmä, joka on suunniteltu nimenomaan yrityskäytössä oleviin puhelimiin.

Valikoimassa olevat puhelimet on pyritty valitsemaan niin, että niissä olisi vähintään yksi soveltuva malli jokaiseen työtehtävään. Insta Groupin alaisuudessa työskentelee mm. automaatioteknologian yritys Insta Automation, jonka työntekijät tarvitsevat työtehtävissään asennustyömailla kestävää puhelinta.

Kaikki yrityksen puhelinasiat hallinnoidaan tilaamisesta palautukseen asti Instan IT-tukiorganisaatiossa. Puhelimet hankitaan kahden vuoden leasingsopimuksella, jonka päätyttyä ne palautetaan toimittajalle tyhjennettyinä.

2.1 Älypuhelinten ohjelmistokokoonpano

Kaikissa yrityksen puhelimissa on tietoturvapolitiikan ohjeistusten mukaisesti virustorjuntaohjelmisto F-Secure Mobile Security. Mikäli käyttäjä jostain syystä poistaa puhelimestaan kyseisen ohjelmiston, tulee se ohjeistuksen mukaan asentaa mahdollisimman pian takaisin. Puhelinasennusten teko Harjavallan tai Oulun toimipaikoilla työskenteleville henkilöille on ollut erittäin haastavaa, koska yrityksellä ei ole ollut käytettävissä etäkäyttöratkaisua asennuksen suorittamiseen. Käyttäjä ei voi asennusta itse tehdä, sillä asennuksessa tarvitaan lisenssiavainta, joka on ainoastaan puhelimia ylläpitävän ICT Supportin tiedossa.

Osassa yrityksen puhelimista on asennettuna myös Mail for Exchange sähköpostiohjelmisto. Sähköpostiohjelman käyttöön vaaditaan tietoturvasyistä myös käyttäjän puhelimeen asennettu erillinen varmenne. Tämän varmenteen käyttö osoittautui haasteelliseksi FromDistancen etähallintaohjelmiston käyttöä testatessa, sillä varmennetta ei voitu asentaa puhelimelle suoraan kyseistä hallintaohjelmaa käyttäen. Tätä ongelmaa käsitellään myöhemmin opinnäytetyössä hieman tarkemmin.

2.2 Tietoturva

Pääosin puolustusteknologian yrityksenä Insta DefSec panostaa laite- ja ohjelmistohankinnoissa suuresti tietoturvaan. Myös mobiililaitteiden kohdalla tietoturva on otettu huomioon.

Edellisessä kappaleessa mainittu F-Secure Mobile Security on yksi osa yrityksen mobiililaitteiden tietoturvaa. Ohjelmaan sisältyy palomuuri, virustorjunta, web-sivujen selaussuoja sekä AntiTheft-ominaisuus, joka on kehitelty laitteen varkaus- ja katoamistilanteita varten.

F-Securen lisäksi puhelimiin on asennettu henkilökohtainen varmenne, joka suojaa käyttäjän sähköpostitiliä ja henkilökohtaisia tietoja. Varmenne asennetaan puhelimiin, joihin on liitetty käyttäjän työsähköposti. Kyseinen varmenne on yrityksen varmennepalvelun kautta luotu mobiilivarmenne, joka luovutetaan käyttäjälle henkilökohtaiseen käyttöön.

Kun puhelimeen on asennettu varmenne sekä sähköpostiasetukset, pakotetaan siihen päälle sähköpostipalvelimelta uusi tietoturvaominaisuus - suojakoodikysely. Suojakoodi lukitsee puhelimen erikseen määritellyn aikajakson kuluessa, mikäli puhelinta ei sinä aikana käytetä. Puhelimen tietoihin pääsee käsiksi ainoastaan syöttämällä oikean suojakoodin. Nokian E75-mallisissa puhelimissa havaittiin 22.3.2011 vakava haavoittuvuus, jonka avulla tämä suojakoodi voitiin ohittaa. Ongelma on kuitenkin korjattu uusimmassa ohjelmistoversiossa. [1]

3 FROMDISTANCE MDM ETÄHALLINTAOHJELMISTON KÄYTTÖ

Tässä luvussa kuvataan FromDistance MDM -ohjelmiston perustyökaluja ja ohjelmiston käyttöä sekä ylläpitäjän että käyttäjän näkökulmasta. Luvussa ovat listattuna myös erään toimittajan palvelumallit FromDistance MDM -tuotekokonaisuudelle.

3.1 Palvelumallit

Tässä työssä pilotoitavan MDM-ratkaisun toimittaja tarjoaa asiakkailleen kolmea erilaista palvelumallia kyseisestä päätelaitehallintapalvelusta. Mallit ovat nimeltään basic, hosted ja hosted managed.

Jokainen palvelumalli sisältää käytännössä samat palvelut, mutta hieman eri tavalla toteutettuina. Kaikkiin malleihin toimitetaan uusimmat päivitykset ja ominaisuudet sopimuksen mukaan, ja käytännössä ainoana erona on se, kuinka itse palvelimia hallinnoidaan.

3.1.1 Basic-palvelumalli

Basic-palvelumallissa palvelut toimivat asiakkaan tiloissa olevilla palvelimilla, ja asiakas vastaa itse laitteiden ja palveluiden ylläpidosta. Ensisijaisesti myös palvelun asennukset - kuten käyttöjärjestelmä, MDM-palvelu ja sertifikaatit - asiakas hoitaa itse. Palveluntarjoajan suorittamat asennukset toimitetaan tiettyä lisämaksua vastaan.

Käytännön näkökulmasta palvelun pystyttäminen käy Basic-palvelumallissa seuraavasti:

1. Palvelun käyttöönotto

    - Asiakas hankkii tarvittavan laitteiston ja perustaa ympäristön

    - Palveluntarjoaja toimittaa tarvittavat lisenssit asiakkaalle

    - Lisäpalveluina palveluntarjoaja toimittaa mm. palvelun käyttöönoton, pää- ja loppukäyttäjien koulutuksen sekä päätelaitteiden ohjelmistopäivitykset

2. Pääkäyttäjät operoivat järjestelmää ja vastaavat konfiguroinneista sekä päivityksistä

3. Palveluntarjoaja antaa pääkäyttäjille tukea palveluaikojen mukaisesti

4. Asiakas vastaa loppukäyttäjien tuesta [2]

3.1.2 Hosted-palvelumalli

Hosted-palvelumallissa palvelut toimivat palveluntarjoajan konesalissa keskitetyssä ratkaisussa. Asiakas vastaa palvelun operoinnista ja loppukäyttäjätuesta.

Basic-malliin verrattuna hosted-mallissa on joitain eroavaisuuksia käytännön ratkaisussa:

1. Palvelun käyttöönotto

    - Palveluntarjoaja perustaa asiakasympäristön

    - Lisäpalveluina palveluntarjoaja toimittaa käyttöönoton asiakkaan tiloissa, pää- ja loppukäyttäjäkoulutukset sekä päätelaitteiden ohjelmistopäivitykset

2. Pääkäyttäjät operoivat järjestelmää ja vastaavat konfiguroinneista

3. Palveluntarjoaja antaa pääkäyttäjille tukea palveluaikojen mukaisesti

4. Asiakas vastaa loppukäyttäjien tuesta

Eroavaisuutena basic- ja hosted-mallilla ovat lähinnä siis itse palvelun fyysinen sijainti ja palvelinten esiasennus. Palveluntarjoaja ei kummassakaan palvelumallissa tarjoa loppukäyttäjille tukea, vaan tuki tarjotaan asiakkaan puolesta. [2]

3.1.3 Hosted managed -palvelumalli

Sekä basic- että hosted-palvelumallit vaativat asiakkaalta jonkin verran teknistä osaamista, sekä mahdollisesti omaa asiakastukea johon loppukäyttäjät voivat ongelmatilanteissa olla yhteydessä. Hosted managed -palvelumalli on suunniteltu yrityksille, joilla on tarve laitehallintapalvelulle, mutta ei esimerkiksi ole mahdollisuutta ylläpitää ja tukea kyseistä palvelua.

Hosted managed -palvelumallissa palvelu tuotetaan palveluntarjoajan konesalissa ja palveluntarjoaja vastaa kokonaisuutena asiakkaan päätelaitteista sisältäen niiden operoinnin sekä loppukäyttäjätuen.

Hosted managed -palvelumallin toimintarakenne on seuraava:

1. Palvelun käyttöönotto

    -Palveluntarjoaja avustaa asiakasta palvelun käyttöönotossa, kun asiakas on määritellyt ympäristön ja sen loppukäyttäjät

    - Lisäpalveluna käyttöönotto asiakkaan tiloissa, pää- ja loppukäyttäjien koulutus sekä päätelaitteiden ja ohjelmistojen päivitys

2. Palveluntarjoajan asiakastuki vastaa palvelun käytöstä

3. Palveluntarjoajan asiakastuki vastaa sekä pää- että loppukäyttäjien tuesta [2]

3.2 Asiakasohjelma FrOMA client

FrOMA client on MDM-ohjelmiston perusohjelma. Kaikilla järjestelmään rekisteröidyillä laitteilla tulee olla asennettuna kyseinen asiakasohjelma, jotta palvelin saa laitteilta ajantasaista tietoa. Nimensä mukaisesti FrOMA client pohjautuu OMA-DM standardiin. Kyseistä standardia käsitellään tarkemmin erillisessä kappaleessa.

Vaikka laitteiden lisäys rekisteriin onkin aluksi puhelinnumeroon perustuvaa, osaa asiakasohjelma raportoida palvelimelle, mikäli laitteen käytössä oleva puhelinnumero vaihtuu. Tämä helpottaa laitteiden ylläpitoa, sillä ohjelmistojen tilaa voidaan seurata, vaikka laitteella käytettäisiinkin eri liittymää.

Asiakasohjelman asennuspaketti voidaan lähettää asiakaslaitteeseen admin-käyttöliittymän kautta. Tällöin käyttäjälle lähetetään tekstiviestitse ohjelman latauslinkki. Kun ohjelma on onnistuneesti asennettu, siirtyy käyttäjän laite automaattisesti admin-käyttöliittymässä rekisteröityneiden laitteiden näkymään. Asiakasohjelman asennus on kuvattu vaiheittain luvussa kuusi (6), jossa käsitellään tarkemmin järjestelmän käyttöä.

3.2.1 OMA DM laitehallintaprotokolla

OMA DM on lyhenne, joka tulee sanoista Open Mobile Alliance Device Management. Open Mobile Alliance on standardikokoelma, joka kerää avoimia standardeja mobiililaitteille.

OMA DM itsessään on laitehallintaprotokolla, joka on määritelty Open Mobile Alliancen standardeihin. Viimeisin versio kyseisestä protokollasta on huhtikuussa 2006 julkaistu versio 1.2.

Kyseinen protokolla on suunniteltu etenkin älypuhelinten sekä kämmentietokoneiden käyttöön. Tärkeimpiä käyttötarkoituksia ovat laitteen yhteyden muodostaminen MDM-palvelimelle, perusominaisuuksien hallinta, asetusten muokkaaminen, ohjelmistopäivitykset sekä vikatietojen kerääminen.

Asetusten muokkaamiseen OMA DM käyttää xml-tiedostoja, jonka sisällä laitteelle toimitetaan suoritettavat komennot. Tällaisia komentoja voivat olla esimerkiksi laitteen ohjelmistopäivitys tai muistikortin pakotettu kryptaus.

Xml-muotoinen komentotiedosto voi olla esimerkiksi seuraavanlainen:

```
<Get>
   <CmdID>2</CmdID>
   <Item>
      <Target>
         <LocURI>./DevDetail/SwV</LocURI>
      </Target>
   </Item>
</Get>
```

Yllä kuvatussa esimerkkikomennossa laitteelta tiedustellaan ohjelmistoversiota, joka löytyy laitteen tiedoista ./DevDetail/SwV -kohdasta. [3][4][5][6]

3.3 Etähallintaohjelma FromVNC client

FromVNC client on FrOMA clientin lisäksi laitteelle asennettava ohjelmisto, joka mahdollistaa laitteen etäkäytön admin-käyttöliittymän kautta. FromVNC perustuu nimensä mukaisesti VNC-tekniikkaan, jota esitellään tarkemmin erillisessä kappaleessa.

FromVNC clientin asennusta vaaditaan myös joidenkin perusasennusta haastavampien ohjelmistomuutosten tekemiseen laitteella. Tällaisia muutoksia ovat esimerkiksi sähköpostiasetusten lisääminen laitteelle.

Kuviossa 1 on esitettynä FromVNC-yhteys admin-käyttöliittymässä. Käyttöliittymä näyttää puhelimen näytön sekä sen fyysiset ominaisuudet. Puhelinta käytetään admin-käyttöliittymän kautta painamalla hiirellä kuvassa olevia puhelimen näppäimiä.

Kuvio 1. FromVNC-yhteys Admin-käyttöliittymässä

Kuten kuvasta voi nähdä, on puhelimen malli tunnistettu Nokia E52:ksi, mutta kyseistä mallia ei ole lisättynä mallipohjiin käyttöliittymässä, joten järjestelmä on valinnut pohjaksi mahdollisimman samankaltaisen puhelinmallin - Nokia E66:n. Vääränlaisesta pohjasta aiheutuu kuitenkin usein ongelmia, sillä malleilla on suuriakin eroja esimerkiksi näppäinten sijoittelussa. Tästä johtuen kaikkia ominaisuuksia ei välttämättä voida hyödyntää ilman oikeanlaista pohjaa eli *skiniä*.

3.3.1 TARM etähallintaoikeus

TARM eli Terminal Access Rights Management on ominaisuus, jolla voidaan seurata esimerkiksi päätelaitteen sijaintia verkossa. TARM on Symbian-käyttöjärjestelmiin liitetty ominaisuus, joka toimii ainoastaan uusimmissa Nokian E-sarjan puhelimissa. Ominaisuus on hyväksyttävä käyttäjän toimesta ennen kuin sitä voidaan laillisesti käyttää. Tämän ominaisuuden käyttöön vaikuttaa henkilön tunnistus- ja paikkatietoihin liittyvä laki, joka määrittää tilanteet, joissa henkilön tai laitteen sijaintia ja tunnistustietoja voidaan seurata kolmannen osapuolen toimesta.

Käyttäjälle päälle kytketty TARM-ominaisuus näkyy puhelimella ruudun yläreunassa pienenä §-merkkinä. Lakipykälä symbolina muistuttaa myös käyttäjää siitä, että ominaisuuden ollessa päällä, voidaan puhelinta ja sen asetuksia seurata erittäinkin tarkasti.

Yrityksen tavoitteena on saada tämä ominaisuus ja sen käyttötarve minimiin, sillä työntekijöiden tunnistustietoja ei haluta edes tahattomasti urkkia ilman erittäin painavaa syytä. Mikäli tietoja pystytään jollain tavalla seuraamaan, on pystyttävä teknisesti seuraamaan myös mitä tietoja kerätään, kenen toimesta, milloin ja mistä syystä.

Jotta ympäristön ylläpitäjiä ja ympäristöä itsessään pystyttäisiin seuraamaan mahdollisimman tarkasti, on kyseinen ympäristö oltava täysin yrityksen hallinnassa. Tämä johtaa siihen, että yritys ei voi ottaa MDM-ohjelmistoa ”avaimet käteen” palveluna miltään palveluntarjoajalta, vaan ohjelmistoon liittyvien palvelinten on käytännössä sijaittava yrityksen tiloissa ja verkossa.

3.4 Admin-käyttöliittymä

Admin-käyttöliittymällä hallitaan kaikkia MDM-ratkaisuun sisällytettyjä ominaisuuksia. Selainpohjainen käyttöliittymä on yksinkertainen ja selkeä, ja sen peruskäytön oppiikin helposti.

Admin-käyttöliittymä sisältää kaikki pääkäyttäjän tarvitsemat toiminnot, ja kyseisen käyttöliittymän kautta ylläpidetään myös koko laitekantaa.

4 FROMDISTANCE MDM ETÄHALLINTAOHJELMISTON OMINAISUUDET

Tässä luvussa on listattuna FromDistancen MDM-ratkaisun ominaisuuksia. Yrityksen kannalta tärkeimmät ominaisuudet on listattu erikseen, ja niitä käydään läpi hieman laajemmin. Muut hyödylliset ominaisuudet sekä tuetut laitealustat on lueteltu erillisissä kappaleissa.

4.1 Tärkeimmät ominaisuudet

Tässä kappaleessa on lueteltuna yrityksen kannalta tärkeimpiä ominaisuuksia, kuten laitteiden ylläpitoon tarkoitettu tietokanta, ohjelmistojen asentaminen puhelimelle, sekä laitteiden etähallinta.

Yritykselle tärkeimpiä ominaisuuksia ovat ne, joita hyödynnetään laiteasennuksissa ja ylläpidossa lähes päivittäin.

4.1.1 Laitetietokanta

Laiterekisterin ylläpitomahdollisuus on yksi MDM-ratkaisun tärkeimmistä ominaisuuksista. Aiemmin yrityksen puhelimia on ylläpidetty käsin useassa eri paikassa, ja näiden listojen ylläpitäminen on yli 500 laitteen kanssa erittäin haastavaa.

Laitetietokannassa on ajantasainen tieto puhelimeen asennetuista ohjelmistoista sekä puhelimen omasta ohjelmistoversiosta. Nämä tiedot auttavat ylläpitäjää selvittämään puhelimella mahdollisesti ilmenneitä ongelmia.

Laitteiden ylläpitäminen yksittäisessä tietokannassa on erittäin helppoa. Laitteita voidaan ryhmitellä tiettyihin ryhmiin, jonka perusteella niille voidaan määritellä erilaisia turvallisuussäädöksiä sekä pakollisia ohjelmistoasennuksia.

4.1.2 Ohjelmistoasennukset

Ohjelmistoasennukset tehdään admin-käyttöliittymän kautta päätelaitteelle. Palvelimella on valmiita asennuspohjia, joita muokkaamalla saadaan yritykselle sopivia ohjelmistopaketteja.

Ohjelmistot asennetaan laitteelle lähettämällä admin-käyttöliittymästä tietty komentosarja puhelimelle. Komentosarja voi sisältää esimerkiksi asennuspaketin lähettämisen, suorittamisen ja poiston päätelaitteelle. Kun asennus on suoritettu, päätelaitetta voidaan ohjata asettamaan ohjelmistolle tietyt asetukset.

4.1.3 Datakäytön ja puheluiden kustannushallinta

Yritysten kustannushallintaa on pyritty tehostamaan ominaisuudella, jolla voidaan seurata käyttäjien puhelinliikennettä erittäinkin tarkasti. Tämä ominaisuus mahdollistaa lähetetyn ja vastaanotetun datamäärän seurantaa, sekä käyttäjän salliessa myös puhelutietoja voidaan tarkkailla.

Kustannushallintaominaisuuksiin kuuluu myös esimerkiksi mahdollisuus estää puhelinten *roaming* eli yhteyden käyttö muualla kuin operaattorin verkossa. Roaming-esto on mahdollista asettaa kaikkiin yrityksen puhelimiin erillisellä politiikalla, johon on määritelty joko sallitut tai estetyt verkot.

4.1.4 Laitteiden etähallinta

Laitteiden etähallinta auttaa päätelaitteiden ylläpidossa huomattavasti. Ylläpitäjä voi tarvittaessa ottaa käyttäjän luvalla yhteyden laitteeseen ja suorittaa esimerkiksi ohjelmiston asetusten tarkistamisen ilman, että käyttäjän tarvitsee toimittaa laitetta mihinkään.

Etähallinnassa käytetään VNC-tekniikkaa, jota käsitellään lisää myöhemmin tässä työssä.

4.1.5 Sijainnin seuranta

Laitteen sijaintia on mahdollista seurata erittäinkin tarkasti laitteen lähettämien GSM- ja GPS-koordinaattien perusteella.

Sijaintitietoja voidaan tarkkailla admin-käyttöliittymän kautta, mutta myös ulkoisiin karttapalveluihin kuten Google Maps-palveluun sijainnin linkittäminen on mahdollista.

Laitteiden seurantaominaisuus vaatii aiemmin tässä työssä mainitun TARM-ominaisuuden sallimista.

4.1.6 Tietoturvan lisäominaisuudet

Lisäturvaa laitteille tuovat erilaiset pakotetut tietoturva-asetukset. Tällaisia asetuksia ovat esimerkiksi yhteysosoitteiden vakiointi, laitteen turvakoodien käytön pakotus, ohjelmistoasennusten estäminen ja salliminen sekä muistilaitteiden salaus.

4.2 Muita ominaisuuksia

Muita hyödyllisiä ominaisuuksia FromDistance MDM-ratkaisussa on useita. Päätelaitehallinnan kautta voidaan hallita laitteiden tiedostoja, ottaa laitteista varmuuskopioita, sekä tarvittaessa tyhjentää laite tai saattaa se käyttökelvottomaksi esimerkiksi katoamistapauksessa.

4.3 Tuetut alustat

Tuettuja alustoja FromDistance MDM-tuotteelle ovat Symbian^3 ja S60, Windows Mobile, BlackBerry, Apple iOS sekä Android.

Kaikki päätelaitehallintapalvelun ominaisuudet ovat tuettuina Symbian-alustoilla, mutta myös Windows Mobile tukee suurinta osaa ominaisuuksista. Muilla käyttöjärjestelmillä tuettuina ovat lähinnä laitekannan ylläpitoon liittyvät inventaario-ominaisuudet sekä laitteen tiedostojärjestelmän muokkaamiseen liittyvät toiminnot, kuten hakemistojen ja tiedostojen lisääminen ja poistaminen. Liitteessä 1 on tarkempi listaus eri alustojen tukemista ominaisuuksista.

5 MOBIILILAITTEIDEN ETÄHALLINTA

MDM-päätelaitehallintaratkaisu käyttää laitteiden etähallinnassa VNC-tekniikkaa, joka mahdollistaa graafisen käyttöliittymän käytön etähallinnassa.

Tässä luvussa käsitellään aiemmissa luvuissa mainittujen FromVNC clientin sekä muiden etäkäyttöominaisuuksien taustalla olevia teknisiä yksityiskohtia, kuten käytettyjä protokollia.

5.1 VNC-tekniikka

VNC on RFB-protokollaa käyttävä tekniikka, joka mahdollistaa työpöydän jakamisen ja täten laitteen etäkäytön graafisen käyttöliittymän kautta. Työpöydän jakaminen tapahtuu verkon yli VNC-palvelimen kautta. Kyseinen palvelin välittää hiiren ja näppäimistön tapahtumat laitteelta toiselle, jolloin käytännössä miltä tahansa laitteelta on mahdollisuus ottaa yhteys mille tahansa laitteelle.

Yksi VNC-tekniikan parhaista eduista onkin sen soveltuvuus useille eri laitealustoille, sillä useat samaan tarkoitukseen käytetyt VPN-palvelut ovat hyvin riippuvaisia käytettävistä tietoverkkoprotokollista sekä käyttöjärjestelmistä.

Peruskomponentit VNC-yhteyden muodostamiseen ovat päätelaitteet, client-ohjelmisto sekä hallintaohjelmisto. Toinen laitteista voi toimia palvelimena ja toinen asiakaslaitteena, mutta yhteys on mahdollista muodostaa myös erillisen palvelimen kautta, johon molemmat laitteista ovat yhteydessä.

FromDistancen FromVNC clientissä yhteys on toteutettu niin, että päätelaitteelle asennettu client odottaa admin-käyttöliittymästä lähetettyä yhteyspyyntöä. Kun yhteyspyyntö on hyväksytty päätelaitteella, muodostuu SSH-yhteys VNC-palvelimelle, joka ohjaa yhteyden selainpohjaiseen admin-käyttöliittymään. [7]

5.1.1 RFB-protokolla

RFB-protokolla on VNC-tekniikan perusta, ja kyseisen protokollan avulla muodostetaan etäkäyttöyhteyksiä laitteille. Viimeisin versio protokollasta on RealVNC Ltd:n kesäkuussa 2007 julkaisema versio RFB 3.8.

RFB toimii laitteiston framebuffer-tasolla, joten sitä voidaan käyttää missä tahansa ikkunointiympäristössä (kuten X11 ja Windows). Framebuffer on laitteella oleva videopiiri, joka suorittaa kuvadataa muistipuskurista.

RFB:tä käytettäessä puhutaan asiakaslaitteista ja palvelimista. Yleensä päätelaite toimii clientinä eli asiakaslaitteena, ja palvelin on laite, jolla otetaan etäyhteys hallittavaan laitteeseen. Kyseisen protokollan perimmäinen ajatus on ollut luoda mahdollisimman yksinkertainen ja yhteensopiva järjestelmä, jolla pystytään hallinnoimaan laitteita laitealustasta riippumatta.

RFB-yhteydet ovat tilattomia, eli palvelin ei seuraa millään tavalla yhteyden tilaa. Mikäli asiakaslaitteen yhteydet jostain syystä katkeavat ja hetken kuluttua palaavat takaisin, osaa palvelin jatkaa siitä mihin se jäi ennen katkosta.

RFB-protokollan graafinen osuus perustuu laitteen näytönohjaimella oleviin pikseleihin. Yksinkertaistettuna RFB-komennot ovat muotoa ”aseta pikseli sijaintiin x,y”.

Kun päätelaitteen ja palvelimen välillä muodostetaan yhteyttä, sovitaan aluksi datan lähettämisen muodosta ja koodauksesta. Muoto ja koodaustapa määrittävät sen, miten pikselitietoa käsitellään. Näihin käsittelyohjeisiin sisällytetään tieto pikseleiden väriarvoista sekä koordinaattien tulkitsemistavasta. [8]

5.1.2 SSH-tunnelointi

SSH-tunnelointi on tietoturvan takia lähes välttämätön lisä VNC-yhteyksien muodostamiseen, sillä VNC itsessään ei ole erityisen tietoturvallinen protokolla. Laitteiden yhteyden muodostamiseen käytettävät salasanat ja salausavain ovat kaapattavissa verkkoliikenteestä. Kun sekä salasana että salausavain ovat tiedossa, voidaan VNC-liikennettä seurata helposti.

SSH:ssa käytetään julkisen avaimen salaustekniikkaa tunnistautumiseen. Yleisin tällaisista salaustekniikoista on RSA, joka on epäsymmetrinen julkisen avaimen salausalgoritmi. RSA-algoritmissa muodostetaan julkinen sekä salainen avain, joita käytetään yhteyden varmentamiseen. Avaimet perustuvat suurten satunnaisten alkulukujen muodostamiseen ja niiden vertaamiseen toisiinsa.

SSH-yhteydet käyttävät liikennöintiin niille määrättyä TCP-porttia 22. Yleisimpiä käyttökohteita SSH:lle ovat palvelinkirjautumiset, suojattu tiedostojen siirtäminen sekä verkkoliikenteen (HTTP) salaaminen.

FromDistancen VNC-ratkaisussa SSH:ta käytetään etäyhteyksien tiedonkulun suojaamiseen. Päätelaitteella muodostetaan SSH-tunneli ja luodaan RSA-salausavaimet yhteyden salauksen muodostamiseksi. [9]

6 TESTIYMPÄRISTÖ

Pilotointia varten palveluntarjoaja pystytti yritykselle ympäristön testauskäyttöä varten. Tässä luvussa käsitellään testiympäristön rakennetta ja käytettävyyttä sekä esitellään eräs testitapaus, jossa arvioidaan FromDistance MDM -tuotteen soveltuvuutta yrityksen käyttöön.

6.1 Testiympäristön rakenne

Yrityksen käyttöön luotu testiympäristö sijaitsi fyysisesti toimittajan konesalissa, ja peruskonfiguroinnit, kuten pääkäyttäjien tunnukset sekä asennustemplatet yleisimmille ohjelmistoille, oli luotu jo valmiiksi ennen käyttöönottoa.

6.2 Testitapaus

Lähtökohtana laiteasennusten testauksille oli, että MDM-ohjelmistolla pystyttäisiin tekemään lähes kaikki tällä hetkellä manuaalisesti tehtävä työ. Tähän asti sekä F-Securen että sähköpostiohjelman asennukset on tehty täysin manuaalisesti.

Testitapauksena on yrityksessä erittäin yleinen puhelinasennus, johon sisältyy F-Securen, mobiilivarmenteen sekä sähköpostiohjelman asentaminen ja asetusten määrittäminen.

Jo testausten alkuvaiheessa havaittiin, että mobiilivarmennetta ei voida asentaa puhelimeen MDM-ohjelmiston kautta, vaan se on asetettava käsin. Itse varmenteen tuonti ja asentaminen tiedostona laitteelle onnistuu, mutta laitteen varmennevarastoa ei voida luoda millään MDM-ohjelmiston tarjoamalla ratkaisulla. Varmenteen täydellinen asentaminen vaatii puhelimen varmennevaraston olemassaoloa, joten tämä asennus vaatii jatkossakin manuaalista työtä.

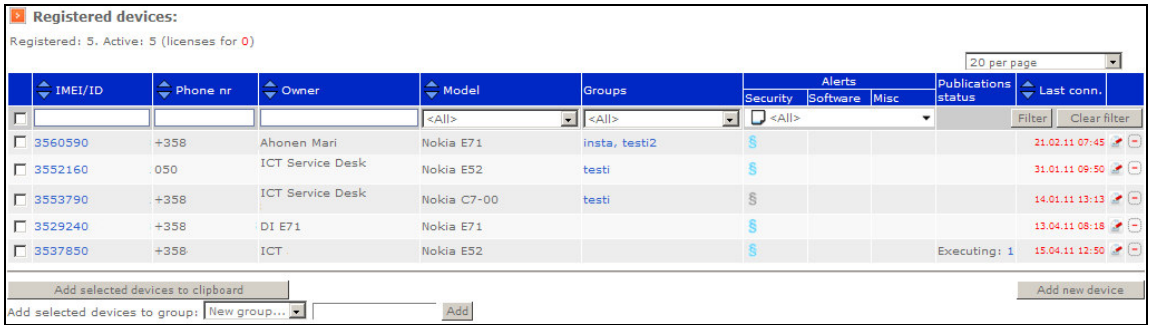
Ongelmana varmenteiden kanssa oli myös se, että kyseinen MDM-ratkaisu ei sisällä suoraan mitään tietokantaa, johon asennettavat varmenteet voitaisiin tallentaa, ja missä niitä voitaisiin ylläpitää.

6.2.1 Laitteen lisääminen laitekantaan

Laitteen voi lisätä laitekantaan usealla eri tavalla. Helpoiten laitteen lisääminen laitekantaan onnistuu pääkäyttäjän toimesta admin-käyttöliittymän kautta. Laitteelle lähetetään aktivointiviesti, jonka mukana tulee latauslinkki asiakasohjelmistoon. Kun ohjelma on asennettu, siirtyy puhelin rekisteröimättömien laitteiden näkymään, josta pääkäyttäjä voi sen lisätä rekisteröityihin laitteisiin.

Laitekannassa on kolme näkymää, joihin on listattu rekisteröidyt, rekisteröimättömät sekä estetyt laitteet. Rekisteröimättömät laitteet ovat laitteita, joihin on asennettu yrityksen FrOMA client, mutta joita pääkäyttäjä ei ole vielä lisännyt järjestelmään. Estetyt laitteet ovat niin ikään pääkäyttäjän lisäämiä laitteita, joiden pääsy laitekantaan on kielletty.

Kun laite on rekisteröity, voidaan siihen ryhtyä asentamaan haluttuja ohjelmia sekä asetuksia. Kuviossa 2 on kuvattuna admin-käyttöliittymän ”Registered users” -näkymä, jossa on listattuna järjestelmään rekisteröidyt laitteet.

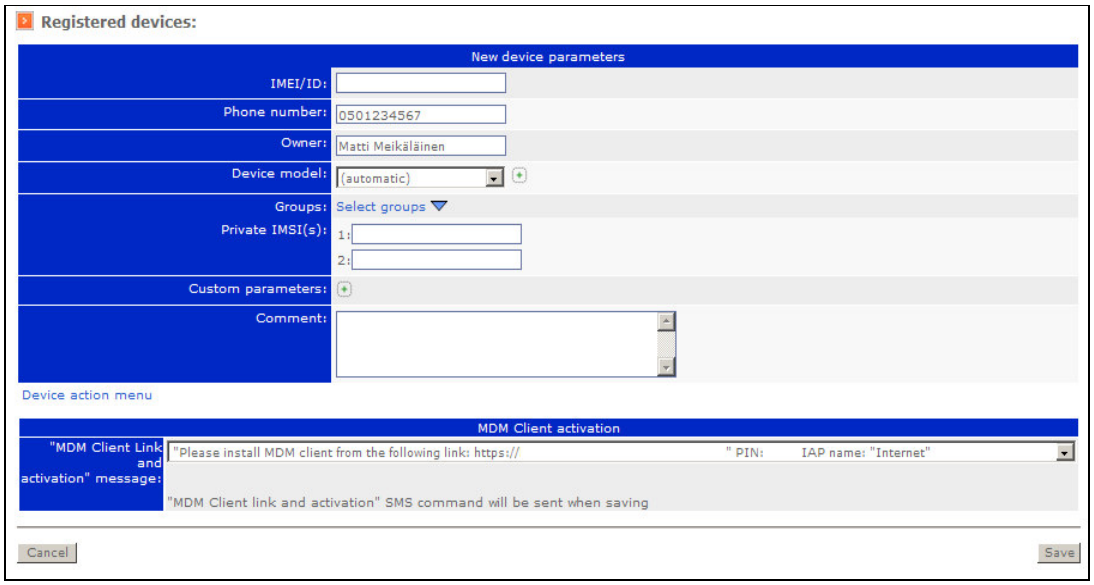


Kuvio 2. Rekisteröityjen laitteiden näkymä admin-käyttöliittymässä

6.2.2 Client-ohjelmien asennus laitteelle

Kuvioissa 3-8 on kuvattu FrOMA clientin asentaminen laitteelle vaiheittain. Ennen kuin asennuksia voidaan tehdä, tulee varmistaa että laitteella on viimeisin ohjelmistoversio. Vanhemmilla ohjelmistoversioilla esimerkiksi Nokian S60-laitteilla on joitain yhteensopivuusongelmia laitehallintaan liittyvien clientien asennuksessa.

Kun puhelimen versio on todettu ajantasaiseksi, ensimmäinen vaihe asennuksessa on laitteen lisääminen laiterekisteriin.

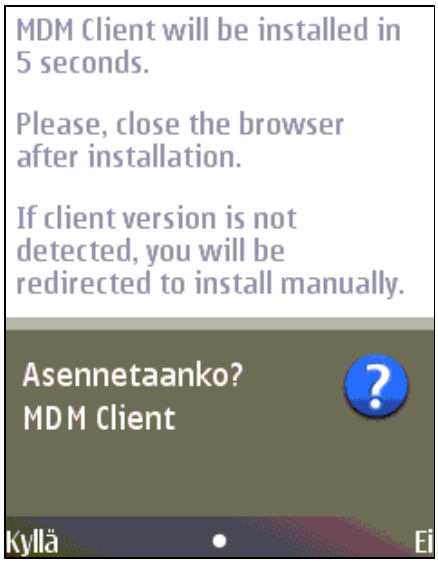


Kuvio 3. Uuden käyttäjän lisääminen Admin-käyttöliittymällä

Käyttäjä saa puhelimeensa tekstiviestin, jossa häntä kehotetaan lataamaan ohjelmisto liitteenä olevasta linkistä. Tekstiviesti sisältää myös käyttäjälle tarpeetonta salattua tietoa, joka pyydetäänkin jättämään huomiotta. Tätä vaihetta kutsutaan *bootstrapping* -vaiheeksi, jossa päätelaite lisätään palvelimelle.

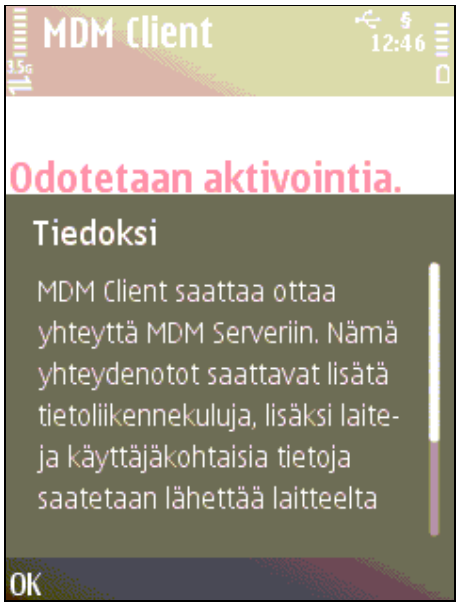
Kuvio 4. Tekstiviestin vastaanottaminen asiakkaan laitteella

Linkki ohjaa päätelaitteen lataamaan asiakasohjelmistoa. Päätelaite varmistaa käyttäjältä, voidaanko ohjelmisto varmasti asentaa.



Kuvio 5. Varmistus ohjelmiston asentamisesta päätelaitteelle

Kun ohjelmisto on asennettu, avautuu ohjelmiston käyttöliittymä päätelaitteelle. Ennen aktivointia käyttäjälle ilmoitetaan, että kyseisellä ohjelmistolla voidaan kerätä käyttäjäkohtaista tietoa laitteelta, ja kyseinen tieto toimitetaan MDM palvelimelle.



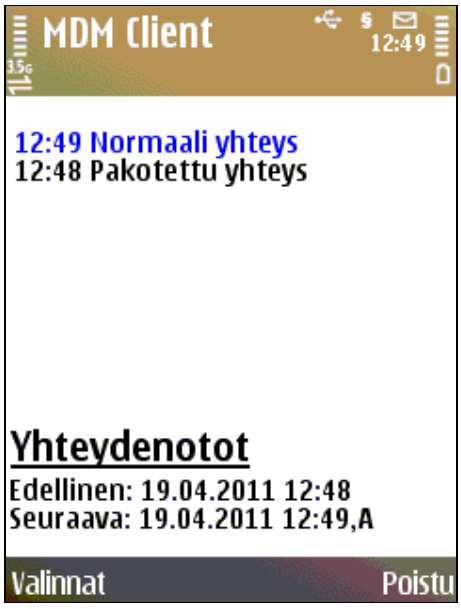
Kuvio 6. Asiakasohjelmiston informaatiokenttä

Käyttäjän hyväksyttyä ohjelmiston käyttöehdot, pyydetään häntä syöttämään ohjelmalle aktivointikoodi, jonka ohjelmiston hallinnoija on toimittanut. Oletuskoodina on 1234, mutta tämä on vaihdettavissa Admin-käyttöliittymän kautta.

Kuvio 7. Aktivointikoodin syöttäminen

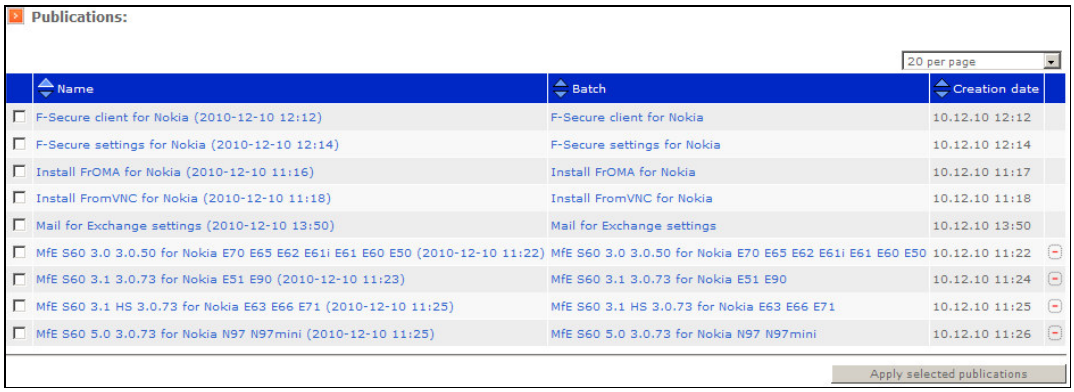
Kun aktivointikoodi on syötetty ja se on mennyt hyväksytysti läpi, yrittää asikaspää ottaa yhteyttä MDM-palvelimelle. Onnistuneen koodin syöttämisen ja yhteysyrityksen jälkeen laitteen ja palvelimen välille on muodostettu luottamussuhde.

Mikäli ohjelmisto ei kuitenkaan itse jostain syystä saa heti yhteyttä, voidaan yhteys avata pakotetusti. Yhteysyritykset näkyvät aikaleimattuina sekä asiakasohjelmistossa että palvelimella. Yhteyttä muodostetaan ajastetusti palvelimelle, joten ohjelma näyttää myös seuraavan yhteysyrityksen ajankohdan.



Kuvio 8. Yhteysyrityksiä asiakasohjelmistolla

Kun FrOMA client on asennettu laitteelle, voidaan siihen asentaa myös etähallintaan käytettävä FromVNC client. FromVNC clientin asennusohjelma voidaan nyt suorittaa päätelaitehallinnan kautta valmiin asennuspohjan kautta, sillä FrOMA clientin avulla laitteelle voidaan suorittaa yksinkertaisia komentoja. Kuviossa 9 on admin-käyttöliittymän ”Publications”-näkymä, jonka kautta laitteille voidaan suorittaa asennuksia.



Kuvio 9. Asennuspohjia admin-käyttöliittymässä

Publications-ominaisuudella voidaan valita laitteelle haluttavat asennuspaketit sekä niiden asennusjärjestys. FromVNC clientin asennuspohja sisältää asennuspaketin siirtämisen laitteelle, clientin asennuksen sekä lopuksi asennuspaketin poistamisen laitteelta. Itse asennuspaketit voidaan siirtää yrityksen palvelimelle, ja kyseinen palvelin voidaan määritellä päätelaitehallintaan asennuspohjiin, jotta laitteille osataan lähettää oikea paketti

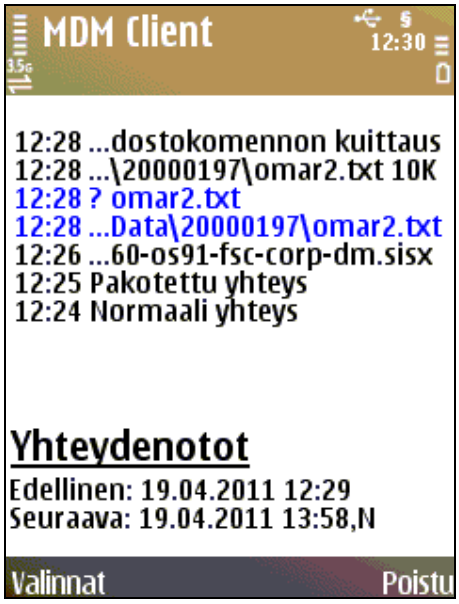
6.2.3 Ohjelmistojen asennus laitteelle

Kun laitteelle on asennettu tarvittavat asiakasohjelmistot, ja se on rekisteröity päätelaitehallintaan, voidaan sille asentaa haluttuja ohjelmia.

Ohjelmistojen asennus laitteelle tapahtuu valmiiden asennuspohjien kautta, kuten FromVNC clientin asennuksessakin. Pääkäyttöliittymän Publications-valikosta valitaan haluttu asennuspohja sekä laite, jolle ohjelma halutaan asentaa.

Puhelimeen asennetaan tässä testitapauksessa F-Secure ja Mail for Exchange clientit sekä niiden erikseen määriteltävät asetukset. Publications-kohdasta valitaan siis järjestyksessä asennuspohjat ”F-Secure client for Nokia”, ”F-Secure settings for Nokia” sekä ”Mail for Exchange settings”. Useissa yrityssarjan puhelimissa on asennettuna valmiiksi Mail for Exchange client, joten sitä ei tarvitse asentaa erikseen laitehallinnan kautta.

Asennusten tilaa voidaan seurata sekä päätelaitteella että admin-käyttöliittymässä. Päätelaitteella asennuksen tila näkyy hieman tarkemmin, sillä admin-käyttöliittymä näyttää ainoastaan suoritettavat asennuspaketit, kun taas FrOMA client päätelaitteella näyttää liikennöntilokissaan asennuksen eri vaiheet. Kuviossa 10 on esitettynä liikennöintiloki F-Securen asennuksen sekä asetusten lisäämisestä laitteelle.

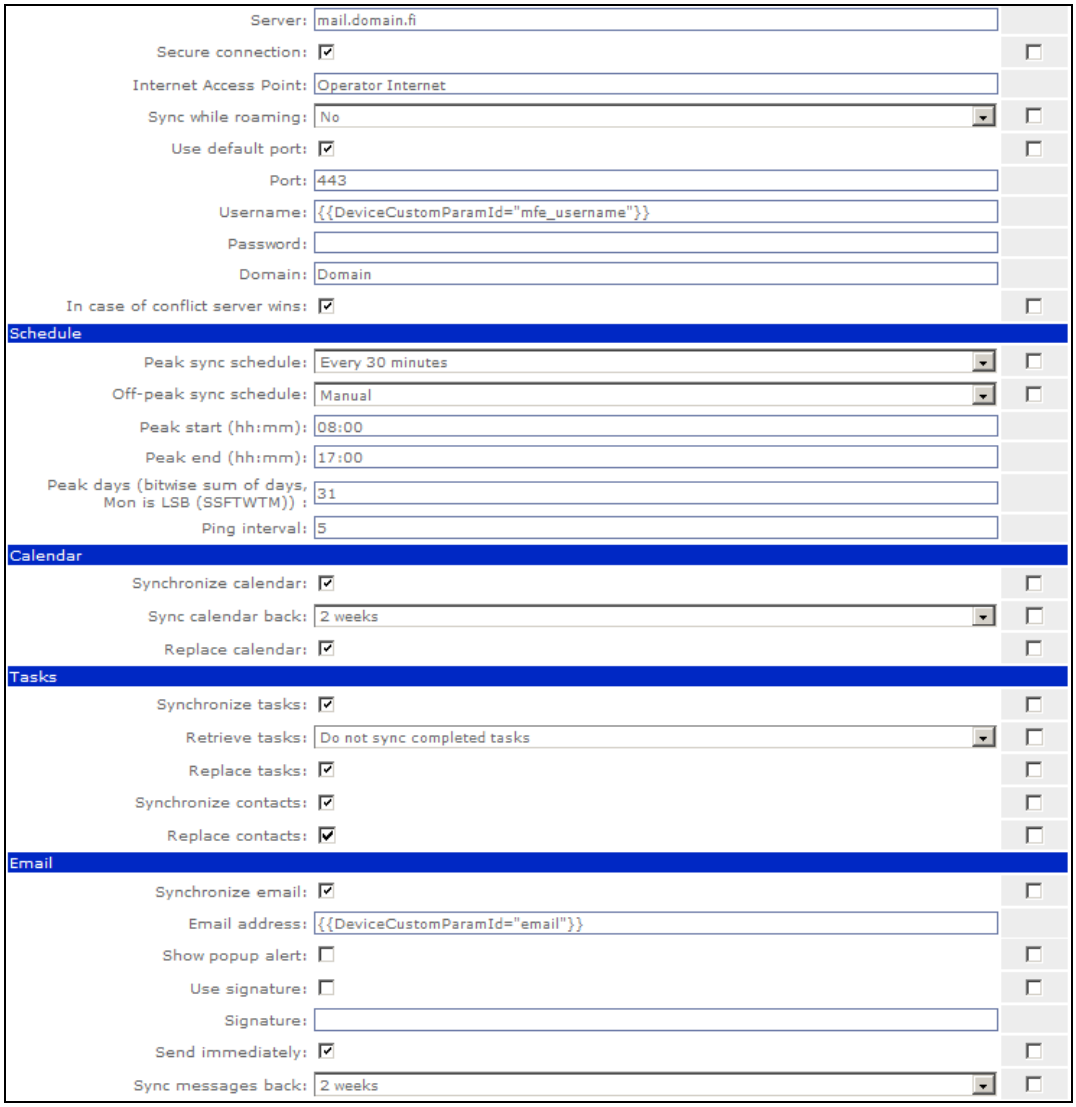


Kuvio 10. F-Securen asennuspohjan suorittaminen päätelaitteelle

Kun F-Secure ja sen asetukset on lisätty laitteelle, jatketaan asennusta mobiilivarmenteen lisäämisellä. Varmenne on asennettava käsin muistikortilta, sillä laitehallinnan kautta ei voida asentaa varmenteita puhelimelle, ellei puhelimen varmennevarastoa ole luotuna valmiiksi.

Mobiilivarmenteen asennuksen jälkeen palataan jälleen käyttämään päätelaitehallinnan admin-käyttöliittymää. Käyttöliittymän ”Batches” -kohdasta voidaan muokata sähköpostiasetuksia ennen niiden lähettämistä puhelimelle. Asennuksia varten olemme kuitenkin luoneet valmiin pohjan, joka asettaa puhelimelle oletusasetukset sähköpostin salasanaa lukuun ottamatta.

Asennuspohjiin voidaan määrittää yhteysasetukset, synkronointiajat sekä synkronoitavat tiedot kuten kalenteri, tehtävät sekä osoitekirja. Kuviossa 11 on esitettynä Mail for Exchangen asennuspohja, johon on lisättynä muutamia perusasetuksia.



Kuvio 11. Mail for Exchangen asetuspohja

Asennuksen viimeisteleminen vaatii vielä käyttäjän syöttämään sähköpostiasetuksiin salasanansa. Tämän jälkeen puhelin on asennettu ja valmis käyttöön. Mikäli ongelmia asennuksissa ilmenee, on ne helppo selvittää FromVNC:n kautta otetun etäyhteyden avulla, jolloin käyttäjän tarvitsee vain hyväksyä yhteyspyyntö laitteita ylläpitävältä taholta.

7 JOHTOPÄÄTÖKSET

Tutkintotyön tavoitteena oli esitellä FromDistance MDM -päätelaitehallintajärjestelmää ja arvioida sen soveltuvuutta yrityksen käyttöön.

Yrityksenä FromDistance on vuonna 2004 suomalaissyntyisen Jouko Vierumäen toimesta perustama kansainvälinen ohjelmistoalan yritys, joka toimii Virossa. Yrityksen muita tuotteita ovat mobiiliin kansalaisjournalismiin tarkoitettu Reportteri-palvelu, ammattimaiseen mobiiliin sisällöntuotantoon tarkoitettu Mobile Professional Reporter -palvelu sekä FromSMS-tekstiviestirajapinta, jota voidaan käyttää esimerkiksi FromDistancen MDM-järjestelmässä tekstiviestien lähettämiseen älypuhelimille palvelimelta.

Kokonaisuutena FromDistancen MDM-ratkaisu on toimiva ja käytännöllinen ratkaisu yritykselle, jolla on tarve hallita suurta määrää puhelimia. Laitteiden etäkäyttö helpottaa laitteiden ylläpitoa sekä ylläpitäjän että käyttäjän näkökulmasta, sillä käyttäjän ei tarvitse toimittaa puhelintaan mihinkään esimerkiksi pelkkien asennusten tarkistamista varten.

Ainoa puuttuva ominaisuus, joka yrityksen käytössä olisi ollut tärkeä, oli varmenteiden etäasennus. Mikäli käsin tehtävä työ haluttaisiin saada karsittua kokonaan pois, tulisi yrityksen harkita jotain muuta ratkaisua sähköpostin turvallisuuden lisäämiseksi. Tällainen vaihtoehto on esimerkiksi matkapuhelinoperaattorin toimittama VPN-ratkaisu, joka sallii ainoastaan yrityksen erikseen rekisteröityjen puhelinten liittämisen yrityksen verkkoon.

Jotta päätelaitehallintaan suunniteltuja ratkaisuja voidaan käyttää yrityksessä tehokkaasti, tulee yrityksen laitevalikoimaa pitää ajantasaisena. FromDistancen ratkaisussa tuettuja laitteita ovat lähinnä uusimmat mallit ja niiden uusimmat ohjelmistoversiot.

Pilotoinnin perusteella FromDistancen päätelaitehallintaratkaisu olisi soveltuva myös Insta Groupin ja sen tytäryhtiöiden laitteiden hallinnointiin. Pilotoinnin jälkeen tarkastellaan ohjelmisto- ja laitehankintojen kustannuksia, niiden kannattavuutta sekä sitä, onko kyseinen ratkaisu riittävän tietoturvallinen yrityksen käyttöön. Näitä asioita ei kuitenkaan ole sisällytettynä opinnäytetyöhön, sillä kyseisten asioiden arviointi tehdään yrityksen hallituksen sekä turvallisuusvastaavien toimesta.

LÄHTEET

[1] CERT-FI haavoittuvuustiedote 043/2011. Luettu 29.3.2011.
http://www.cert.fi/haavoittuvuudet/2011/haavoittuvuus-2011-043.html

[2] Palveluntarjoajan toimittama MDM päätelaitehallintaratkaisun palvelukuvaus [Luottamuksellinen]

[3] MobilityDojo, OMA-DM One Step at a Time. Luettu 9.4.2011.
http://mobilitydojo.net/2009/05/07/oma-dm-one-step-at-a-time/

[4] Wikipedia, Open Mobile Alliance. Luettu 9.4.2011.
http://en.wikipedia.org/wiki/Open_Mobile_Alliance

[5] Wikipedia, OMA Device Management. Luettu 9.4.2011.
http://en.wikipedia.org/wiki/OMA_Device_Management

[6] Xml-muotoisia komentotiedostoesimerkkejä. Luettu 11.4.2011.
http://msdn.microsoft.com/en-us/library/ms889554.aspx

[7] Wikipedia, Virtual Network Computing. Luettu 14.4.2011.
http://en.wikipedia.org/wiki/Virtual_Network_Computing

[8] RFB 3.8 Protocol Standard. Luettu 14.4.2011.
http://www.realvnc.com/docs/rfbproto.pdf

[9] Wikipedia, Public-key cryptography. Luettu 18.4.2011.
http://en.wikipedia.org/wiki/Public-key_cryptography

Palveluntarjoajan kanssa käydyt keskustelut pilotoitavaan ohjelmistoon liittyen vuosina 2010-2011

FromDistance, MDM Client v1.85 Security Guide [Luottamuksellinen]

FromDistance, MDM Admin Guide [Luottamuksellinen]

FromDistance, MDM User Guide [Luottamuksellinen]

FromDistance MDM Feature Matrix. Luettu 12.4.2011.
http://www.fromdistance.com/datasheets/Fromdistance_MDM_Features.pdf

LIITTEET

FROMDISTANCE FEATURE MATRIX LIITE 1: 1(4)

• = Supported — = Not applicable for the platform	Symbian^3 & S60	Windows Mobile	BlackBerry	iOS	Android
Inventory					
IMEI	•	•	•	•	•
IMSI	•	•	•	• (ICCID)	•
Roaming status	•	•	•	•	•
Battery status	•	•	•	•	•
Firmware	•	•	•	•	•
Hardware	•	•	•	•	•
Manufacturer	•	•	•	•	•
Language	•	•		•	
Free space of device memory	•	•	•	•	•
Free space of removable media	•	•	•	—	•
Access points settings	•	•	•	•	
Installed software name/ID/version	•	•	•	•	
Network information	•	•	•	•	
GPS	•	•	•	•	
Call logs	•	•			•
Data traffic usage (GPRS/3G and WLAN)	•	•	—	•	
File system management					
Create folder	•	•	•	—	•
Copy file to device	•	•	•	—	•
Copy files/folders from device	•	•	•	—	•
Delete files	•	•	•	—	•
Delete folders	•	•	•	—	
Launch file	•	•		—	•
Move files from device	•	•	•	—	•
Restore files to device	•	•	•		

LIITE 1: 2(4)

• = Supported — = Not applicable for the platform	Symbian^3 & S60	Windows Mobile	BlackBerry	iOS	Android
Configuration management					
Registry operations	—	•	—	—	—
Country information	•	•		•	•
AT commands	•			—	
Network mode	•				
Browser bookmarks	•	•			
SyncML data synchronization settings	•				
Home screen applications (OMA DM)	•		—	—	
Key shortcuts (OMA DM)	•		—	—	
OMA device management settings	•	•	—	—	
VoIP settings	•		—	—	
SIP settings	•		—	—	
Internet Access Points					
CSD settings	•		—		
GPRS settings	•	•	—	•	
WLAN settings	•	•	—	•	
WLAN settings/advanced WLAN settings	•	•	—	•	
Default access points	•	•	—		
Email					
Email settings for POP/IMAP	•	•		•	
Email data roaming setting	•	•		•	
ActiveSync settings	—	•		•	
Lotus Notes Traveler settings	•	—	—		
Corporate Exchange account settings	•	•	—	•	
Seven Email settings	•		—		

• = Supported — = Not applicable for the platform	Symbian^3 & S60	Windows Mobile	BlackBerry	iOS	Android
Security					
Device reboot	•	•			
Device wipe/detonate	•	•			
USB blocking	•				
Enable/disable device autolock	•	•		•	
Enable/disable keypad autolock	•				
Certificate management	•	•		•	
Encryption settings	•	•		•	
Enable/disable Bluetooth	•	•			
Enable/disable hidden Bluetooth	•	•			
Enable/disable camera	•	•		•	
Enable/disable device encryption	•	•		•	
Enable/disable the installation of user's own applications	•	•		•	
Enable/disable locked and user unchangeable/addable settings	•	•			
Security policy settings for SIM card change	•	•			
Alerts for policy breaches	•	•			
Platform-specific functionalities	Nokia ADM policies			Restrictions (iTunes, YouTube, explicit content, network games, application purchase and install...) Clear passcode Jailbreak-status	
• = Supported — = Not applicable for the platform	Symbian^3 & S60	Windows Mobile	BlackBerry	iOS	Android
Backup and restore					
Contacts	•	•		•	
Calendar	•	•			
Email messages	•	•			
Tasks	•	•			
Notes	•	•			—
Files and folders	•	•			
Multimedia	•	•			
SMS inbox	•	•	—	—	
Bookmarks	•				
Software management					
Silent installation	•	•	—	•	
Installation parameters	•	•		—	
Stop/kill application	•	•	—		
Start application	•	•		•	
Install/update/remove native applications	•	•		•	SD card only
Install/update/remove Java applications	•	•		—	—
Monitor application	•	•		•	
Alerts for application breaches	•	•			
Mandatory application list	•	•		•	
Application black list	•	•		•	
Corporate policy management	•	•		•	
Remote desktop access				—	

LIITE 1: 4(4)

• = Supported — = Not applicable for the platform	Symbian^3 & S60	Windows Mobile	BlackBerry	iOS	Android
Software configuration					
F-Secure Mobile Security	•		—	—	
Pointsec encryption	•	—	—	—	
Psiloc connect	•	—	—	—	
Platform-specific applications	Siemens HiPath				
	Alcatel-Lucent UC				
	Nokia CC for Cisco				
	Nokia VPN				
Exportable reports					
Application report	•	•	•		
Model report	•	•	•	•	•
Memory report	•	•	•	•	•
Firmware version report	•	•	•	•	•
Data traffic usage (GPRS/3G and WLAN) report	•	•			
Bluetooth details report	•	•			
Network report	•	•	•		•
Location report	•	•	•	•	•
GPRS/3G report	•	•		•	
Logs report	•	•	•		•
Backup and restore report	•	•		•	