MOBIILILAITTEIDEN KESKITETTY HALLINTA YRITYSVERKOSSA

Ammattikorkeakoulun opinnäytetyö

Tietotekniikan koulutusohjelma

Riihimäki, 3.5.2012

Jaakko Hartikainen

HAMK
HÄMEEN AMMATTIKORKEAKOULU

RIIHIMÄKI
Tietotekniikan ko
Tietotekniikka

TIIVISTELMÄ

Tekijä Jaakko Hartikainen **Vuosi** 2012

Työn nimi Mobiililaitteiden keskitetty hallinta yritysverkossa

TIIVISTELMÄ

Tämän opinnäytetyön tarkoituksena oli perehtyä saatavilla oleviin ns. keskitetyn hallinnan ratkaisuihin iOS – ja Symbian – alustoille, sekä selvittää näistä soveltuvin ratkaisu toimeksiantajan, Suomen Lehtiyhtymä Oy:n käyttöön. Myös olemassa olevia tietoturvariskejä pohdittiin. Opinnäytetyön aihe saatiin toimeksiantajan tarpeesta siirtää olemassa oleva mobiililaitekanta lähitulevaisuudessa keskitetyn hallinnan piiriin. Hallintajärjestelmän käyttöönoton toteutus rajattiin kuitenkin toimeksiantajan vastuulle.

Opinnäytetyössä selvitettiin Apple MDM – ja OMA DM – protokollien sekä hyödyntävien keskitetyn hallinnan ohjelmistojen toimintaa. Taustatietoa kerättäessä käytettiin laite- ja ohjelmistovalmistajien dokumentaatiota, teknisiä WWW – resursseja sekä kirjallisuutta. Käytännön kokeita suoritettiin toimeksiantajan iPhone 4 – lainapuhelimella sekä Windows Server 2008R2 – virtuaalipalvelimella.

Havaittiin, että ns. pilvipalvelut edustavat keskitetyn hallinnan ohjelmistojen tulevaisuutta niin teknisten seikkojen kuin kustannustehokkuudenkin kannalta. Ensisijaisena vaihtoehtona päädyttiin suomalaiseen CapriCode SyncShield – ohjelmistoon sekä toissijaisena vaihtoehtona Fiberlink Maas360 – ohjelmistoon. Keskitetyn hallinnan käyttöönotto mahdollistaa yrityksen tietoturvapolitiikan valvonnan myös laajentuvassa mobiililaiteympäristössä. Haittaohjelmatilanteen perusteella suositellaan Symbian – laitekannan migraatiota tietoturvan kannalta ajantasaisempaan Windows Phone 7.5 - käyttöjärjestelmään.

Avainsanat MDM, mobiilikäyttöjärjestelmät, SaaS, tietoturva

Sivut 33 s. + liitteet 1 s.

HAMK
UNIVERSITY OF APPLIED SCIENCES

RIIHIMÄKI
Degree Programme in Information Technology

Author Jaakko Hartikainen **Year** 2012

Subject of Bachelor's thesis Mobile device management in a corporate environment

ABSTRACT

The objective of the thesis was to investigate and to review the most suitable options of Mobile Device Management (MDM) software for iOS and Symbian platforms. Suomen Lehtiyhtymä Oy, the commissioner of the thesis, is currently planning a mass deployment of MDM to all of its existing mobile devices. Software was reviewed in terms of security and requirements set by the commissioner. Recommendations are based on in-depth research results, but the actual deployment of MDM was out of the scope of this thesis.

Relevant protocols, such as Apple MDM, OMA – DM and MDM software were investigated using first-party technical documentation, online resources and literature. Practical testing was completed using iPhone 4 hardware and Windows Server 2008R2 in a virtualized environment.

Cloud–based MDM services were observed to be superior in cost-efficiency and ease of configuration when compared to traditional on-premise delivery. Capricode SyncShield, a Finnish MDM solution was considered the primary choice. Fiberlink Maas360, which was also tested extensively in action, is the second option. Deployment of MDM allows existing security policies to be enforced in a growing mobile device environment. The Symbian platform was found to be massively targeted by malware and other attacks, so migration of existing Symbian phones into the more modern Windows Phone 7.5 was recommended.

Keywords MDM, mobile operating systems, SaaS, security

Pages 33 p. + appendices 1 p.

TERMIT JA LYHENTEET

APNS	Apple Push Notification Service, välityspalvelu viestin välittämiseen mobiililaitteille
CA	Certificate Authority, sertifikaatteja myöntävä organisaatio tai vastaava
CSR	Certificate Signing Request, käyttösertifikaatin allekirjoituspyyntö
iOS	Laitevalmistaja Applen kaupallinen käyttöjärjestelmä mobiililaitteille
Jail-breaking	iOS - käyttöjärjestelmän rajoituksien poisto ohjelmallisesti
MDM	Mobile Device Management, yleinen nimitys mobiililaitteiden keskitetylle hallinnalle
NDES	Network Device Enrollment Service, Microsoftin toteutus SCEP:stä Windows Server – alustalle
OTA	Over-the-air programming, mobiililaitteen ohjelmiston tai asetusten päivittäminen ilman fyysistä yhteyttä
OMA-DM	Open Mobile Alliance Device Management, mm. Symbian – käyttöjärjestelmässä käytetty keskitetyn hallinnan arkkitehtuuri
PKI	Public Key Infrastructure, julkisen avaimen infrastruktuuri, tietoturvakokonaisuus digitaalisten salausavaimien ja identiteettien käyttöön
SCEP	Simple Certificate Enrollment Protocol, Cisco Systemsin sertifikaattien käyttöönottoprotokolla
TLS	Transmission Layer Security, tiedonsalausprotokolla
UDID	Unique Device Identifier, iOS – laitteen yksilöllinen tunniste

SISÄLLYS

1 JOHDANTO

1.1 Tavoitteet ja työn tarkoitus

Tehokkaiden mobiililaitteiden, kuten Apple iPad – taulutietokoneiden ja erilaisten älypuhelimien yleistyminen yritysympäristössä asettaa haasteita niiden ylläpitoon ja valvontaan. Käyttöönotettujen laitteiden määrän kasvaessa useihin satoihin yksiköihin on ylläpitohenkilökunnan ja käyttäjien ajan sekä yrityksen resurssien säästämiseksi otettava käyttöön keskitetyn hallinnan ohjelmisto. Koska työntekijöiden käyttöön annetut mobiililaitteet ovat usein mukana myös vapaa-ajalla, tietoturvariskit suurenevat huomattavasti. Mikäli puhelin häviää käyttäjältään tai se varastetaan, on tärkeää että yrityksen järjestelmänvalvoja voi nopeasti ja vaivattomasti pyyhkiä laitteen sisältämät tiedot tai estää sen käytön kokonaan. Langattoman yhteyden jatkuvan käytön takia on otettava huomioon myös erilaiset siirtotiehen liittyvät hyökkäykset. Mobiililaitteiden käyttöjärjestelmien lisääntynyt kompleksisuus ja ominaisuuksien määrä asettaa haasteita turvalliseen käyttöön.

Opinnäytetyön tarkoituksena on perehtyä saatavilla oleviin etähallintaratkaisuihin sekä iOS- että Symbian- mobiilialustoille ja selvittää näistä soveltuvin ratkaisu toimeksiantajan, Suomen Lehtiyhtymä Oy:n käyttöön. Suomen Lehtiyhtymä Oy:n mobiililaitekantaa laajennetaan lähitulevaisuudessa huomattavasti mm. iPhone – puhelimilla ja iPad – taulutietokoneilla. Näin ollen käyttöön on otettava mahdollisimman tietoturvallinen ja toimintavarma ohjelmisto, jolla voidaan automatisoida uusien laitteiden käyttöönotto ja olemassa olevien hallinta. Myös havaittuihin tietoturvaongelmiin ja -uhkiin otetaan kantaa, mutta niiden käytännön ratkaiseminen on rajattu aiheen ulkopuolelle. Keskitetyn hallinnan ohjelmiston käyttöönoton toteutus jätetään toimeksiantajan henkilökunnan tehtäväksi.

1.2 Toimeksiantaja

Suomen Lehtiyhtymä Oy on Suomen viidenneksi suurin lehtikustantaja ja painopalvelujen tuottaja. Yrityksen palveluksessa on yhteensä noin 500 työntekijää ja omistuksessa 22 sanomalehteä sekä 11 yhteistyölehteä (Suomen Lehtiyhtymä Oy, 2010). Mobiilaitekanta muodostuu noin 70 kappaleesta Nokian E7 ja C7 Symbian – yrityspuhelimia sekä 120 kappaleesta Apple iPhone 4 – puhelimia. Jälkimmäisten määrää on tarkoitus lisätä lähitulevaisuudessa ainakin 50 kappaleella. Tämän lisäksi johtohenkilökunnalla on käytössään 15 kappaletta Apple iPad 2 – taulutietokoneita (Nieminen, sähköpostiviesti 15.12.2011).

Toimeksiantajan oma tietohallintohenkilökunta ottaa iOS – laitteet käyttöön Applen iTunes – ohjelmistolla. Symbian – laitteilla käytetään Nokian Ovi

Suitea. Toimeksiantajan edustaja on todennut tämän käytännön riittämättömäksi laitteiden määrän lisääntyessä ja tietohallinto – osaston henkilökunnan muiden työtehtävien kasvaessa. Työntekijöiden tyypillinen puhelimen käyttö koostuu sähköpostin lukemisesta ja lähettämisestä FirstClass Mobile – asiakasohjelmalla. Myös kalenterin synkronointi on tärkeä ominaisuus.

1.3 Vaatimukset

Etähallinnan vähimmäisvaatimukset sovittiin toimeksiantajan yhteyshenkilön kanssa opinnäytetyön suunnittelun yhteydessä. Ehdottomasti vaadittuja etähallinnan kautta käytettäviä ominaisuuksia ovat puhelimen/laitteen etätyhjennys (suorituskykyongelmien ehkäiseminen), synkronointiasetusten määrittäminen, sähköpostiasiakasohjelman asennus, laitteen sisällön varmuuskopiointi sekä palautus/kloonaus (kloonaamalla voidaan laitteeseen viedä valmiiksi yrityksen kaikki puhelinnumerot). Etähallintapalvelimen alustan valintaan ei ollut erityisiä kriteerejä. Toimeksiantajan käytössä on oma palvelintila oheisjärjestelmineen. Virtualisoitua käyttöönottoa tai pilvipalvelun käyttämistä (SaaS) ei suljettu pois. Muita erityisvaatimuksia ei toimeksiantaja tässä vaiheessa asettanut (Nieminen, sähköpostiviesti 15.12.2011).

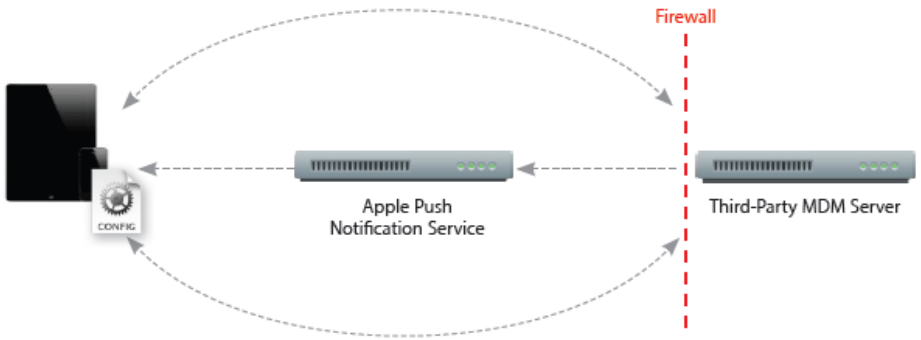
2 HALLINTASOVELLUSPROTOKOLLAT

2.1 Tietoperusta ja käsitteistö

Opinnäytetyössä tarkastelun kohteena olevien mobiililaitteiden keskitettyyn hallintaan liittyy keskeisesti kaksi tekniseltä toteutukseltaan olennaisesti toisistaan poikkeavaa protokollaa, joilla pyritään samaan lopputulokseen. Molempia tarvitaan opinnäytetyön tavoitteen saavuttamiseksi, sillä Apple Mobile Device Management (MDM), on nimensä mukaisesti käytettävissä vain iOS – laitteilla, ja vastaavasti Symbianilla keskitetty hallinta voidaan toteuttaa vain Open Mobile Alliance Device Managementilla (OMA-DM). Applen iOS tukee myös vanhempaa hallintamallia, jossa etukäteen luodut profiilit ladataan hallintapalvelimelta käsin puhelimella (Faas 2010, 1). Tämä malli havaittiin kuitenkin riittämättömäksi opinnäytetyön vaatimuksien kannalta.

2.1.1 Apple MDM ja Push Notification Service – arkkitehtuuri

Apple Mobile Device Management (MDM) on iOS – laitteille suunniteltu hallinta-arkkitehtuuri, joka mahdollistaa suuren laitemäärän hallitsemisen resurssitehokkaasti ja turvallisesti. Apple MDM otettiin käyttöön iOS - käyttöjärjestelmän version 4 myötä. Aiemmista iOS – versioista poiketen MDM – arkkitehtuuri on osa käyttöjärjestelmän ydintä ja eliminoi siten tarpeen erillisille apusovelluksille (Phifer, 1-2). Pohjimmiltaan Apple MDM käyttää samaa profiilipohjaista tekniikkaa kuin yksityiskäyttäjille suunnattu iPhone Configuration Tool, ja mahdollistaa kolmannen osapuolen hallintapalvelimen käyttämisen saumattomasti yritysympäristössä (Edge 2010, 217 - 218). Tiedonpäivitykseen mobiililaitteen ja hallintapalvelimen välillä käytetään Apple Push Notification Serviceä (APNS). Push Notification Service on mobiililaitteelle viestejä välittävä palvelu, joka säästää laitteiden resursseja ja yksinkertaistaa integraatiota yrityksen omaan verkkoon (Kuva 1). Sen tarkoituksena on informoida mobiililaitetta asetusten päivitystarpeesta.



Kuva 1. Havainnekuva Push Notification Servicen toiminnasta (Apple 2011).

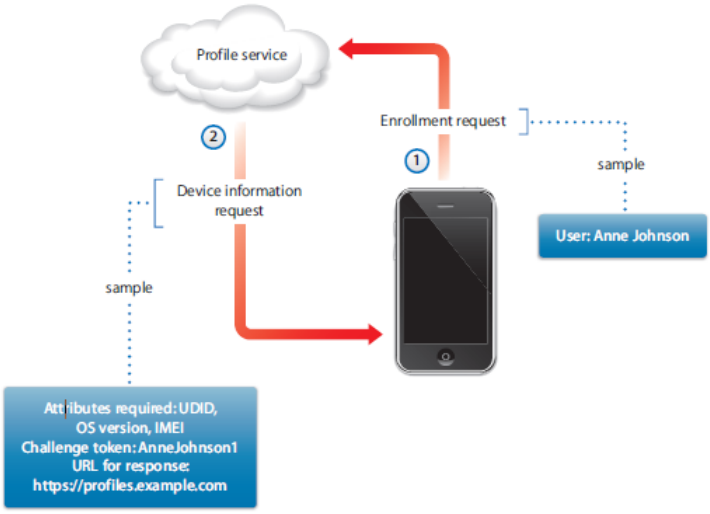
Esimerkkinä hallintapalvelimen ”Third Party MDM Server” halutessa kommunikoida mobiililaitteen kanssa lähetetään APNS:n TCP - portin 2195 kautta yhteysilmoitus (notification). Mobiililaite yhdistää tämän jälkeen TLS – salatulla HTTPS - yhteydellä suoraan hallintapalvelimeen ja suorittaa profiilin päivitystoimenpiteet, vaikkapa yrityksen VPN – palvelimen asetuksien vaihdon. Mikäli laite ei ole tavoitettavissa tai tapahtuu muunlainen virhetilanne, APNS käyttää ns. feedback – palvelua ilmoittaakseen hallintapalvelimelle virhetilanteesta (Apple 2011, 2-3). Kuvan 1 tilanteessa oletetaan, että hallintapalvelin on suojattu palomuurilla. Tällöin on otettava huomioon APNS:n tarvitsemat porttiasetukset, jotka on listattu taulukossa 1.

Taulukko 1. Push Notification Servicen käyttämät portit.

Portti / liikenteen suunta	**Käyttö**
2195/TCP, lähtevä	Hallintapalvelimen viestit APNS:lle
2196/TCP, saapuva	Feedback - palvelun liikenne
5223/TCP, lähtevä	Hallintapalvelimen viestit APNS:lle (WLAN)

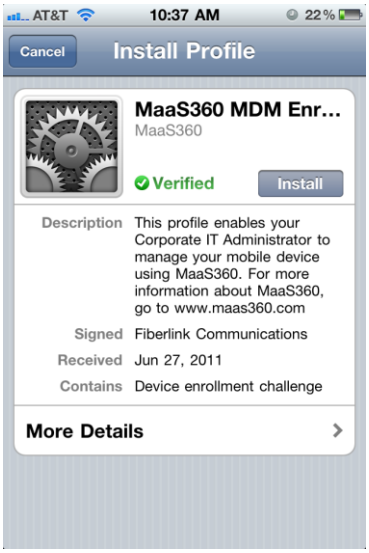
Kolmannen osapuolen hallintapalvelinta ensimmäistä kertaa käyttöönotettaessa tarvitaan useita sertifikaatteja. Välityspalvelun käyttöä varten on hankittava käyttösertifikaatti (Apple 2012). Applen tietoturvakäytännöistä johtuen allekirjoituspyyntö, (Certificate Signing Request, CSR), lähetetään ensin valitun kolmannen osapuolen hallintapalvelimen toimittajalle. Allekirjoitettu sertifikaatti rekisteröidään Apple ID – tunnuksia käyttämällä Applen Push Certificates – portaalissa, minkä jälkeen Push Notification Service on käytettävissä. Sertifikaatin luominen on havainnollistettu luvussa 3.3.1. Asetusprofiilien salaamiseen ja yksilöintiin käytetään laitekohtaisia sertifikaatteja (Device Certificate), joiden luonnissa käytetään Cisco Systemsin kehittämää Simple Certificate Enrollment Protocol (SCEP) – protokollaa (Edge 2010, 218). Laitekohtaisilla sertifikaateilla saavutetaan useita etuja. Niillä voidaan lukita asetusprofiilitiedostot vain tiettyihin mobiililaitteisiin, sekä estää käyttäjiä ylikirjoittamasta haluttuja asetuksia tahallaan tai vahingossa.

Kun verkkoasetukset ja sertifikaattipalvelin (joko erillisenä komponenttinaan tai osana valmista hallintapalvelinta) ovat kunnossa, suoritetaan hallittavien laitteiden kirjaaminen hallintapalvelimelle langattomasti (Over-the-air enrollment). Kirjaaminen on kertaluontoinen prosessi jossa edellytetään käyttäjän hyväksyntää etähallinnan käyttöön (Edge 2010, 245). Ensimmäisessä vaiheessa käyttäjälle lähetetään tyypillisesti SMS- tai sähköpostiviesti, joka sisältää hyperlinkin profiilipalveluun (Profile Service). Profiilipalvelu on tyypillisesti integroitu osaksi kolmannen osapuolen hallintapalvelinta, mutta sitä voidaan käyttää myös erillisenä kokonaisuutenaan. Ensimmäisessä vaiheessa käyttäjät tunnistetaan joko yksinkertaisella HTTP – autentikoinnilla tai esimerkiksi olemassa olevilla LDAP – tai Active Directory - tunnuksilla (Kuva 2).



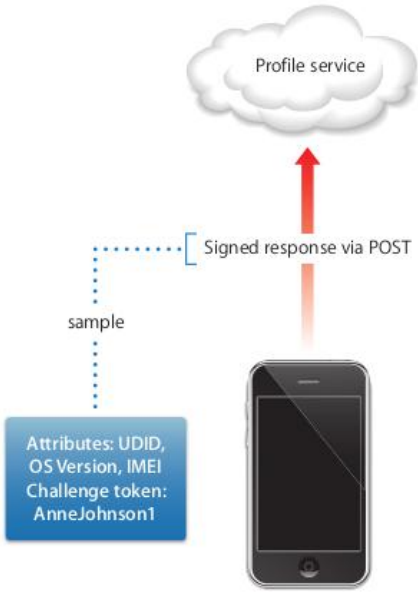
Kuva 2. Kaavio kirjaamisen ensimmäisestä vaiheesta.

Kun käyttäjän kirjauspyyntö (1, enrollment request) on autentikoitu, profiilipalvelin lähettää vastauksen (2, device information request). Vastukseen sisältyy alustava profiilitiedosto, ja mobiililaitetta vaaditaan lähettämään tyypillisesti UDID – tunniste, käyttöjärjestelmän versionumero, sekä mahdollisesti muita tietoja, kuten IMEI – koodi. Vastaukseen on myös liitetty koodi (challenge token), jolla käyttäjä tunnistetaan jatkossa kirjaamisprosessin aikana. Käyttäjän tai järjestelmänvalvojan on hyväksyttävä alustava profiilitiedosto painamalla Install – nappia (Kuva 3). Tämän jälkeen käyttäjäsyötettä ei tarvita jatkossa lainkaan.



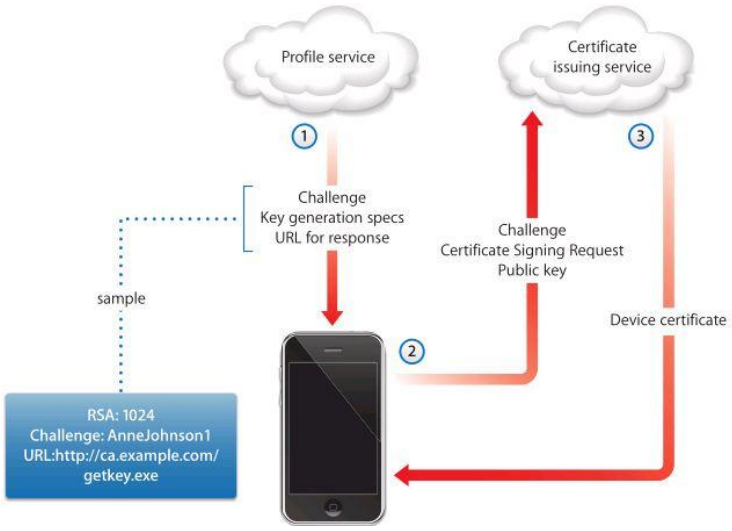
Kuva 3. Esimerkki Maas360 – profiilin käyttöönotosta.

Toisessa vaiheessa mobiililaite vastaa profiilipalveluun HTTP:tä käyttämällä edellä mainituilla tiedoilla (Kuva 4) ja käyttää allekirjoituksessa laitteen sisäistä sertifikaattia (built - in identity).



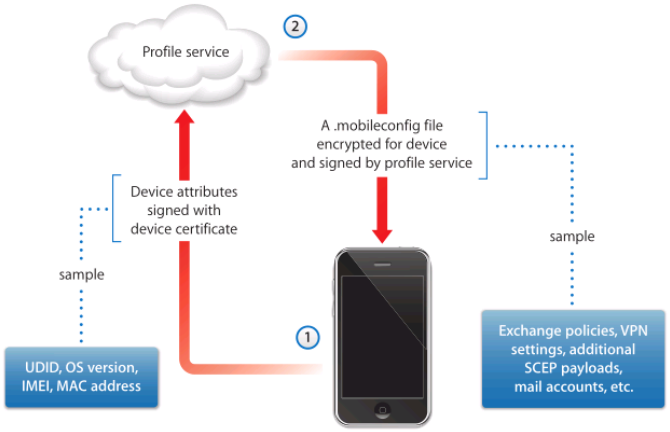
Kuva 4. Kaavio kirjaamisen toisesta vaiheesta.

Kolmannessa vaiheessa luodaan laitekohtainen sertifikaatti. Profiilipalvelu lähettää mobiililaitteelle käytettävän algoritmin tyypin (esimerkiksi RSA), käyttäjätunnisteen edellisestä vaiheesta (challenge token) sekä SCEP:n tarvitseman osoitteen (1). Tiedonsiirto sertifikaatin myöntäjälle (Certificate Authority) kohdissa 2 ja 3 tapahtuu SCEP:llä. (Kuva 5).



Kuva 5. Kaavio kirjaamisen kolmannesta vaiheesta

Kirjaamisen neljäs ja viimeinen vaihe on lopullisen, allekirjoitetun konfiguraation pyytäminen profiilipalvelulta (Kuva 6). Kohdassa 1 lähetetään samat tiedot kuin ensimmäisessä vaiheessa, mutta tällä kertaa laitekohtaisella sertifikaatilla allekirjoitettuna. Kun profiilipalvelu on näin varmistunut laitteen ja käyttäjän identiteetistä, lopullinen asetusprofiili, .mobileconfig, salataan, allekirjoitetaan ja lähetetään mobiililaitteelle kohdassa 3. Profiili asentuu mobiililaitteeseen automaattisesti.



Kuva 6. Kaavio kirjaamisen neljännestä vaiheesta.

2.1.2 Simple Certificate Enrollment Protocol (SCEP)

Simple Certificate Enrollment Protocol on Cisco Systemsin kehittämä protokolla, jota voidaan käyttää sertifikaattien myöntämiseen ja jakeluun turvallisesti erilaisille verkkolaitteille. SCEP käyttää julkisen avaimen infrastruktuuria (PKI) perustuen PKCS#7 ja PKCS#11 – standardeihin, joita ei käsitellä tarkemmin tässä opinnäytetyössä. Protokolla on suunniteltu skaalautuvaksi ja hyödyntämään jo olemassa olevaa verkkoinfrastruktuuria (Cisco Systems 1998, 1). Alustariippumattomuuden ansiosta SCEP – palvelinohjelmistona voidaan käyttää vaatimuksien mukaan joko avoimen lähdekoodin ratkaisuja (OpenSCEP) tai Microsoftin Windows Server – palvelimien Network Device Enrollment Service - palvelua käyttämällä (Microsoft 2010). Jälkimmäisen käyttöön vaaditaan Windows Serverin Enterprise – versio, tai Windows Server 2008 R2.

SCEP – protokollassa on määritelty kolme erityyppistä ilmentymää (”entity”). Certificate Authority (CA) myöntää sertifikaatit, joilla varmistetaan julkisten avaimien omistajien identiteetti järjestelmässä. CA:na voidaan käyttää yrityksen olemassa olevaa järjestelmää, esimerkiksi Windows Server – ympäristössä Certificate Servicesiä. Registration Authority (RA) on SCEP:n terminologiassa palvelinta vastaava ilmentymä, joka käsittelee protokollan mukaisia viestejä HTTP – muodossa. Asiakas (client, end entity) on mobiililaite tai muu verkkolaite, jonka identiteetti SCEP:llä pyritään varmistamaan. Tiedonsiirto tapahtuu yksinkertaisilla HTTP GET – pyynnöillä. Esimerkiksi luvussa

2.1.1 käsitellyssä mobiililaitteen kirjaamisen kolmannessa vaiheessa (Kuva 4) käytetään SCEP – protokollan viestiä GetCACert. Tällöin kyseessä on Certificate Signing Request (CSR), jolla pyydetään CA:lta varmennettua laitekohtaista sertifikaattia. Mikäli virhetilanteita ei synny, CA vastaa niin ikään HTTP – muodossa lähettämällä laitekohtaisen sertifikaatin X.509 - formaatissa (Cisco Systems 1998, 1-3; 8-9). Optimaalisissa olosuhteissa SCEP:n toiminta on mobiililaitteen käyttäjälle täysin näkymätöntä. SaaS – pohjaisissa palveluissa kappaleessa 2.1.1 kuvattu sertifikaattien jakelu on käytännössä integroitu palvelinpuolella toimivaksi ja keskitetyn hallinnan pääkäyttäjän ei tarvitse konfiguroida sitä erikseen.

2.1.3 Open Mobile Alliance Device Management (OMA - DM)

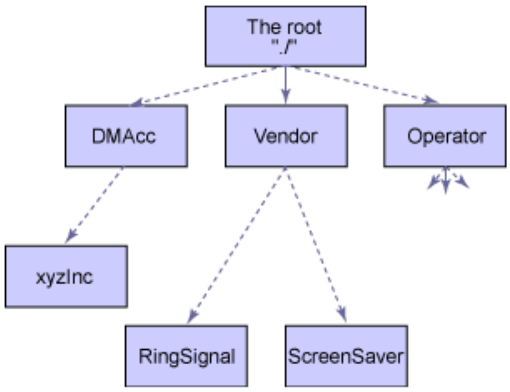
Open Mobile Alliance Device Management on nimensä mukaisesti Open Mobile Alliance – järjestön kehittämä protokolla sen tukemien mobiililaitteiden hallinnointiin. Kehitystyön alullepanija oli alun perin The SyncML Initiative Ltd., joka sulautettiin myöhemmin mukaan Open Mobile Alliance – järjestöön. Open Mobile Allianceen kuuluu joukko laitteisto – ja ohjelmistovalmistajia, kuten Microsoft, Oracle Corporation, IBM, Nokia, Motorola, yms. OMA-DM – protokollan viimeisin versio on 1.2, jonka julkaisu tapahtui vuonna 2006 (Open Mobile Alliance 2012, Architecture: 1-2). Symbian – käyttöjärjestelmän, Windows Mobilen ja muiden OMA-DM:ää tukevien laitteiden markkinaosuuksien pienentyessä protokollan kehitysvauhti on hidastunut huomattavasti ja se ei ole toiminnoiltaan yhtä kattava kuin esimerkiksi Applen MDM. Protokollan tarkoituksena on mahdollistaa tuettujen mobiililaitteiden etähallinta, päivittäminen sekä asetusten muutokset. Yksinkertaisella palvelin-asiakasohjelma – mallilla toimivaa protokollaa voidaan käyttää joko puhelimen langattoman datayhteyden kautta (HTTP, Over-the-air) tai kiinteällä yhteydellä (USB, RS-232). Langattoman yhteyden käyttö palomuurilla varustetussa verkossa edellyttää taulukossa 2 esitettyjen porttien avaamista.

Taulukko 2. OMA – DM:n käyttämät porttiasetukset.

Portti / liikenteen suunta	**Käyttö**
500/UDP, saapuva ja lähtevä	OMA – DM push - viestit
4500/UDP, saapuva ja lähtevä	IPsec - tunnelointi

OMA – DM – protokollan viestit välittyvät XML – formaatissa. Järjestelmä koostuu hallintapalvelimesta (server) sekä mobiililaitteista, joilla voi olla yksi tai useampi asetuspiste (node). Asetuspisteet on järjestetty OMA – DM – laitteissa ns. hallintapuuksi (management tree, Kuva 7). Asetuspisteitä voivat olla muun muassa mobiililaitteen globaalit asetukset tai ajonaikainen ympäristö (run-time environment). Tyypillisen OMA – DM – hallintasession toiminta on kaksivaiheinen. Ensimmäisessä vaiheessa (setup phase) hallintapalvelin lähettää mobiililaitteelle herätysviestin (alert). Herätysviestit välitetään mobiililaitteelle UDP – portin 500 välityksellä (Taulukko 2). Tämä tapahtuu luonnollisesti vain jos hallintapalvelin itse aloittaa tiedonsiirron. Tämän jälkeen mobii-

lilaitteelta vaaditaan yksinkertaista autentikointia ja mobiililaitteen tunnistamista (Apple MDM:sta poiketen OMA – DM – protokolla itsessään ei tue laitekohtaisia sertifikaatteja). Sekä palvelin että mobiililaite siirtyvät käyttämään tässä vaiheessa HTTP:tä. Tunnistetiedot sisältävät tyypillisesti mobiililaitteen uniikin tunnisteen (DevId) sekä käyttöjärjestelmän tyypin ja versionumeron. Hallintapalvelin vastaa omilla vastaavilla tiedoillaan, mikäli autentikointi onnistui.



Kuva 7. Esimerkki OMA – DM – yhteensopivan laitteen hallintapuusta.

Varsinaiset päivitys- ja hallintatoimenpiteet tapahtuvat toisessa vaiheessa (management phase). OMA – DM tukee useita käskyjä, joilla muokataan hallintapuussa olevien asetuspisteiden arvoja. Asetuspisteet sisältävät avain – arvo – pareja, joita voidaan lisätä, poistaa, kopioida tai muokata.

3 KESKITETYN HALLINNAN OHJELMISTOT

3.1 Yleinen luokittelu

Keskitettyyn hallintaan tarkoitettujen ohjelmistojen valmistajina on sekä tunnettuja tietoturvallisuus- ja ohjelmistoyrityksiä (esim. Symantec ja HP), että pelkästään yhden tuotteen ympärille rakentuvia yrityksiä. Oulussa toimiva Capricode on ainoa suomalainen valmistaja. Markkinoilla olevia valmiita keskitetyn hallinnan ohjelmistoja tarjotaan pääasiassa kolmena erityyppisenä ratkaisuna:

- Software-as-a-Service (SaaS)
- On-premise deployment
- Appliance deployment, virtualized deployment

SaaS – mallissa hallintapalvelin voi sijaita fyysisesti missä päin maailmaa tahansa (ns. pilvipalvelu). Mobiililaitteet ja pääkäyttäjä(t) ottavat hallintapalvelimeen yhteyden WAN – verkon ylitse, ja palvelun toimittaja vastaa ylläpidosta ja huoltotoimenpiteistä. Päivitykset ja korjaukset asennetaan asiakkaalle läpinäkyvästi. Asiakkaana toimiva taho maksaa tyypillisesti hankinnan yhteydessä kiinteän käyttöönottomaksun, ja kuukausittaisen maksun riippuen hallittavien laitteiden kokonaismäärästä. Asiakkaan kannalta suurin hyöty on käyttöönoton yksinkertaisuus ja kertainvestoinnin pieni määrä verrattuna tilanteeseen, jossa perinteinen palvelinlaitteisto hankitaan, asennetaan ja ylläpidetään itse (Microsoft 2006). Haittapuolena on kuitenkin täydellinen riippuvuus palvelun toimittajasta sekä tietoliikenneyhteyksien toimivuudesta. Opinnäytetyön tutkimusta suoritettaessa havaittiin, että SaaS – palveluiden kustannustaso on käytännössä aina muita ratkaisuja huokeampi.

On-premise deployment, asiakkaan tiloihin asentaminen on perinteinen ratkaisu. Mobiililaitteet ottavat palveluun yhteyden WAN – tai LAN – verkon ylitse. Asiakas on itse vastuussa palomuuriasetuksista ja sovelluksen asentamisesta palvelimeen. Käyttöönottokustannukset voivat olla yllättävän korkeat, mikäli olemassa olevaa laitesalia tai muuta fyysistä ympäristöä ei ole. Huolto – ja päivitystoimenpiteet ovat pääasiassa asiakkaan vastuulla, ellei erillistä (yleensä maksullista) palvelua ole sopimuksessa määritelty.

Virtualisointiympäristön ja erityisten sulautettujen järjestelmien (appliance) hyödyntäminen ohjelmistojen toimittamisessa on uudehko suuntaus. Erilaisten laitteistopohjaisten palomuuri – ja VPN – ratkaisujen valmistajat, kuten Cisco Systems ovat alan pioneereja, mutta esimerkiksi tässä opinnäytetyössä käsitelty AirWatch tarjoaa dedikoitua palvelinjärjestelmää omalle etähallintaratkaisulleen.

Kaikilla opinnäytetyössä tarkastelluilla etähallintaratkaisuilla oli virallinen tuki kolmelle kirjoitushetkellä markkinaosuudeltaan suurimmalle mobiilikäyttöjärjestelmälle:

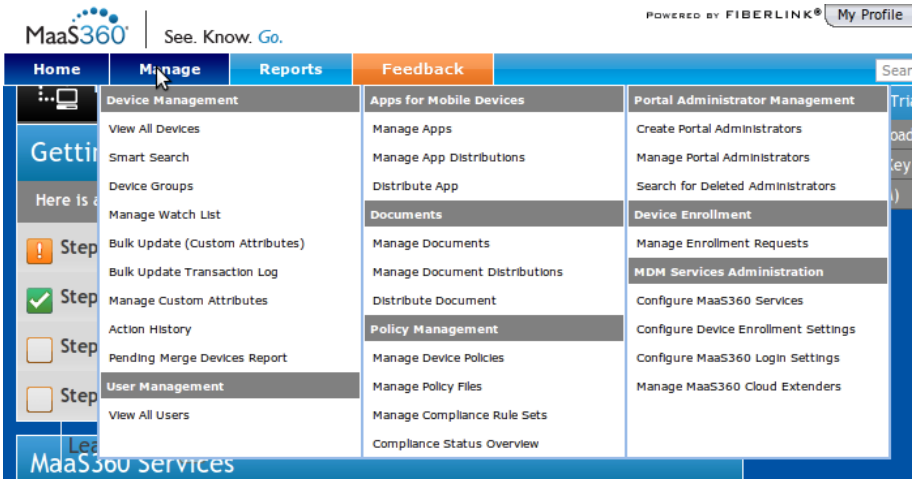
Operating System	4Q11 Units	4Q11 Market Share (%)
Android	75,906.1	50.9
iOS	35,456.0	23.8
Symbian	17,458.4	11.7
Research In Motion	13,184.5	8.8
Bada	3,111.3	2.1
Microsoft	2,759.0	1.9
Others	1,166.5	0.8

Kuva 8. Mobiilikäyttöjärjestelmien markkinaosuudet vuoden 2011 viimeisen neljänneksellä (Gartner Inc. 2012).

Opinnäytetyön tavoitteen kannalta varteenotettavista etähallintaratkaisujen toimittajista koostettiin alustava luettelo (Liite 1). Yhtä poikkeusta lukuun ottamatta etähallintaratkaisujen pääasiallisena alustana käytetään Windows Server 2008R2:aa. Vanhentunutta 2003 – versiota tuki vain Symantec Mobile Management. Toimeksiantajan vaatimuksen käyttöalustasta ja tuetuista mobiilikäyttöjärjestelmistä täyttävät yhdeksästä vaihtoehdosta kaikki muut paitsi HP Mobile Management, LANDesk Mobility Manager ja McAfee. Nämä ratkaisut karsittiin pois tutkimustyön alkuvaiheessa, eikä niitä käsitellä enempää tässä opinnäytetyössä.

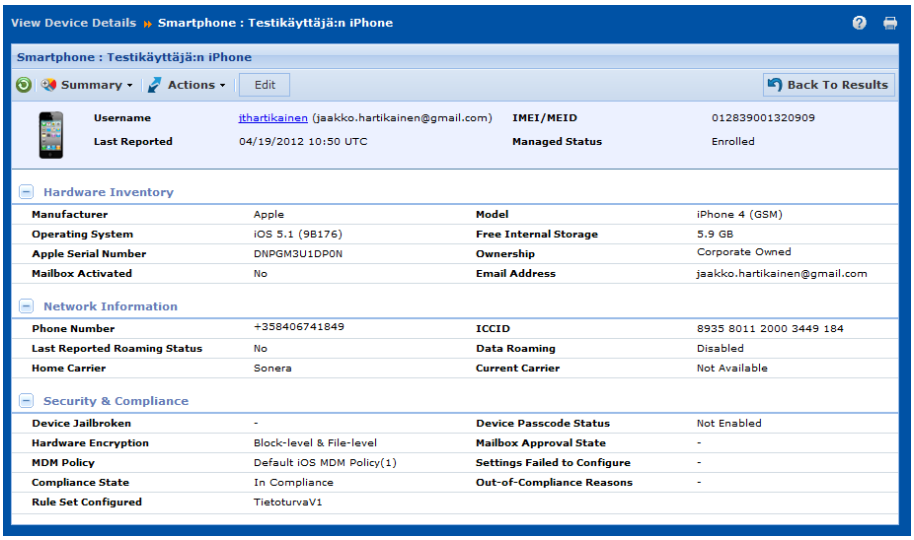
Hinnoittelu on käyttötarkoituksen mukaan vaihtelevaa. Tarkkoja tietoja ei kaikilta luettelon valmistajilta tutkimustyötä tehdessä saatu, koska tämä olisi vaatinut varsinaisen tarjouspyynnön toimeksiantajan lähettämänä. Sähköpostitse saatiin selvitettyä kuitenkin hinnoitteluperusteet. Jokaista hallinnan piirissä olevaa mobiililaitetta kohden maksetaan lisenssimaksu. Kuukausittaisen (n. 3 – 5 € per laite) maksun sijasta osa valmistajista tarjoaa myös ns. pysyvää lisenssimaksua (perpetual license). Kiinteät käyttöönottokustannukset vaihtelevat riippuen siitä, asennetaanko laite asiakkaan tiloihin.

3.2 Perustoiminnot

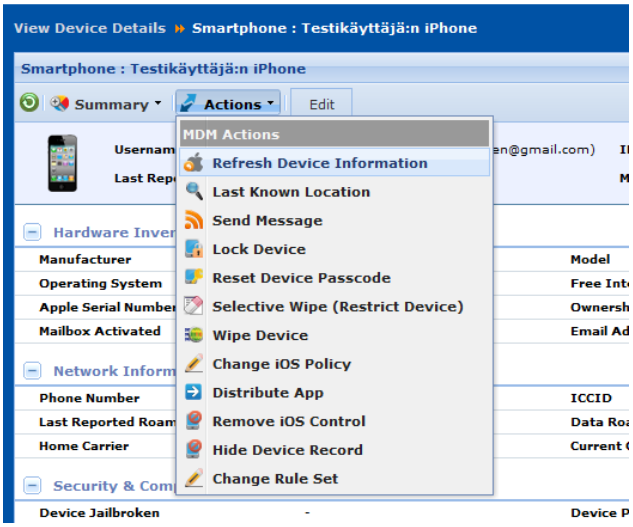


Kuva 9. Esimerkki keskitetyn hallintajärjestelmän päävalikosta (Maas360).

Käytännössä kaikki opinnäytetyötä varten tutkitut keskitetyn hallinnan ohjelmistot sisältävät HTML/JavaScript - pohjaisen hallintakäyttöliittymän, jonka kautta kaikki keskeiset toiminnot suoritetaan (Kuva 9). Erillinen työasemaan asennettavaa sovellus on kuitenkin saatavilla joillekin ohjelmistoille (Liite 1). Selainpohjaisena hallinta onnistuu Windows, Macintosh ja Linux/Unix – ympäristöissä. Opinnäytetyön tutkimustyön puitteissa ei ollut aikarajoitteen takia mahdollista tilata ja koekäyttää erikseen jokaista hallintaratkaisua, joten lähdemateriaalina käytettiin myös valmistajien omaa teknistä dokumentaatiota. Tarkkailtavat ja hallinnan piirissä olevat mobiililaitteet voidaan luokitella organisaatioyksikön, mobiililaitteen tyypin tai vaikkapa maantieteellisen sijainnin perusteella (GPS). Yksittäistä mobiililaitetta tarkastellessa nähdään esimerkiksi akun tila, verkkosignaalin vahvuus ja laitteen vapaan muistin määrä. Yhdelle tai useammalle tavoitettavissa olevalle mobiililaitteelle voidaan suorittaa toimenpiteitä, kuten etätyhjennys, etätuki ja tiedostonhallinta. (Kuvat 10 ja 11).

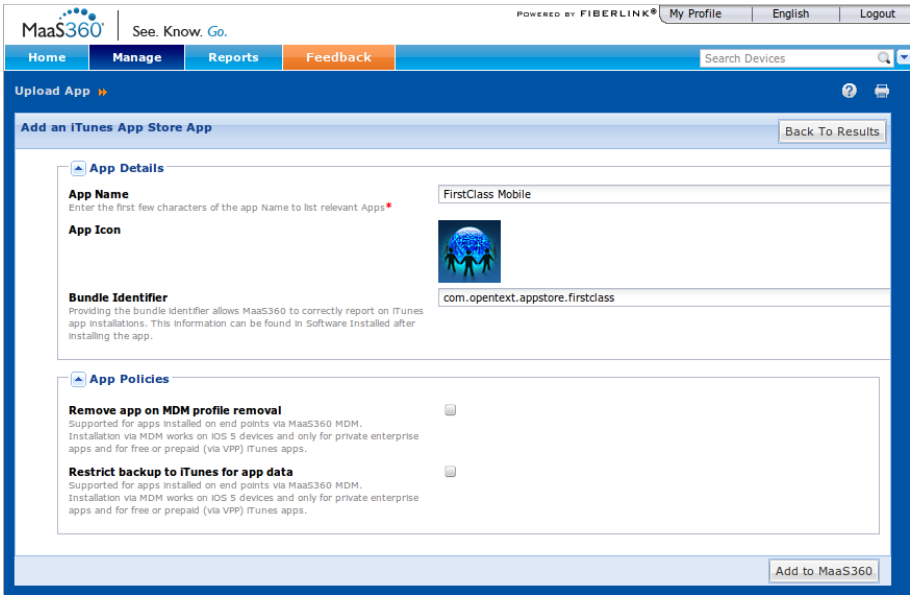


Kuva 10. Yksittäisen mobiililaitteen tarkastelu Maas360:ssa.



Kuva 11. Laitekohtaiset toiminnot.

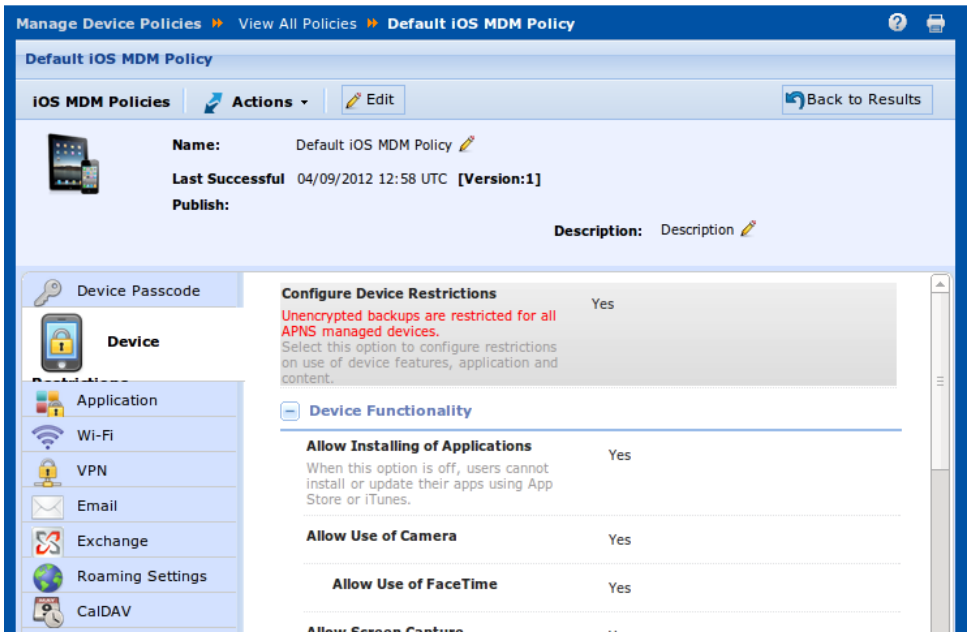
Hallintakäyttöliittymä kykenee tuottamaan pääkäyttäjälle raportteja, jolloin esimerkiksi poikkeukset tietoturva – asetuksissa tai luvaton SIM – kortin vaihtaminen voidaan havaita nopeasti. Mikäli käyttäjän (työntekijän) asema ja käyttöoikeudet vaihtuvat yrityksessä, kaikkiin tietyn käyttäjän mobiililaitteisiin voidaan soveltaa uutta käytäntöä (policy).



Kuva 12. Sähköpostisovelluksen lataaminen Maas360 – hallintaan.

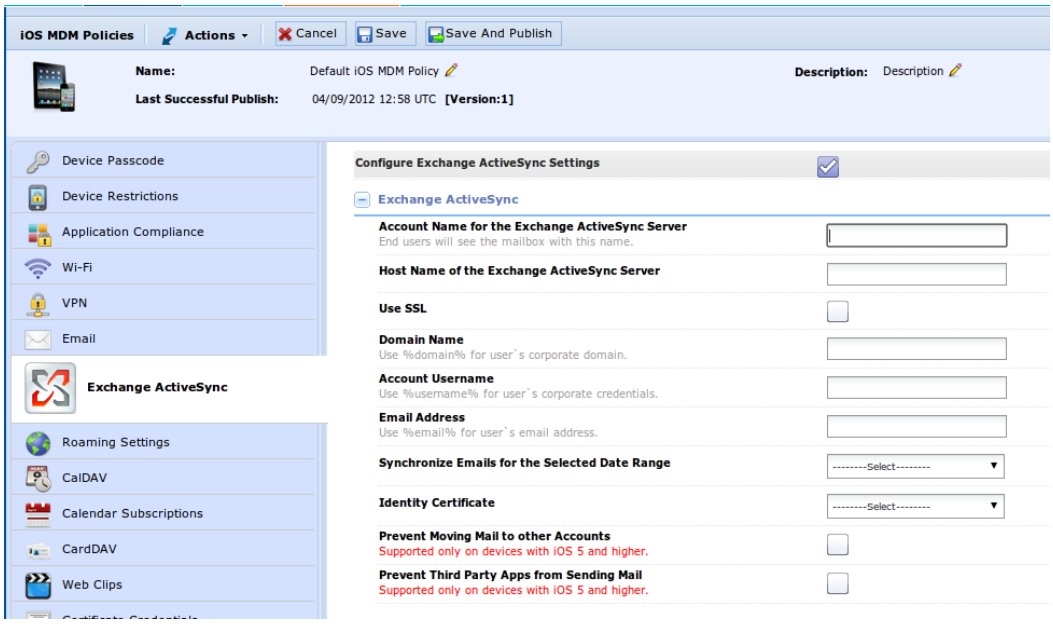
Sovelluksien asentaminen keskitetysti tapahtuu lataamalla asennustiedosto hallintakäyttöliittymään kohdelaitteesta riippuen App Storesta, Android Marketista tai yrityksen omalta palvelimelta (Kuva 12). iOS – laitteille voidaan asettaa lisärajoituksia, kuten varmuuskopioinnin rajoittaminen iTunes – palve-

luun sekä sovelluksen automaattinen poistaminen, kun laite poistetaan keskitetyn hallinnan piiristä.



Kuva 13. Käytännön muokkaaminen Maas360:ssa.

Mobiililaitteisiin voidaan soveltaa erilaisia käytäntöjä, jotka vastaavat Group Policy – ratkaisua Windows Serverissä. Käytäntöä voidaan soveltaa yhteen tai useampaan laitteeseen ja se sisältää kaikki yksityiskohtaiset asetukset ja rajoitukset (Kuva 13). Maas360:ssa käytäntöjä voi määritellä mobiililaitteiden käyttöjärjestelmä- tai ryhmäkohtaisesti. Käytäntöjen avulla on mahdollista yhtenäistää mobiililaitteiden tietoturva – asetukset yrityksen muiden laitteiden kanssa. Esimerkiksi opinnäytetyön toimeksiantajan vaatima FirstClass Mobile – yhteyssovellus käyttää kalenterin ja yhteystietojen synkronointiin Exchange ActiveSync – palvelinta. Nämä asetukset voidaan määrittää etukäteen kaikille tarvittaville laitteille (Kuva 14).



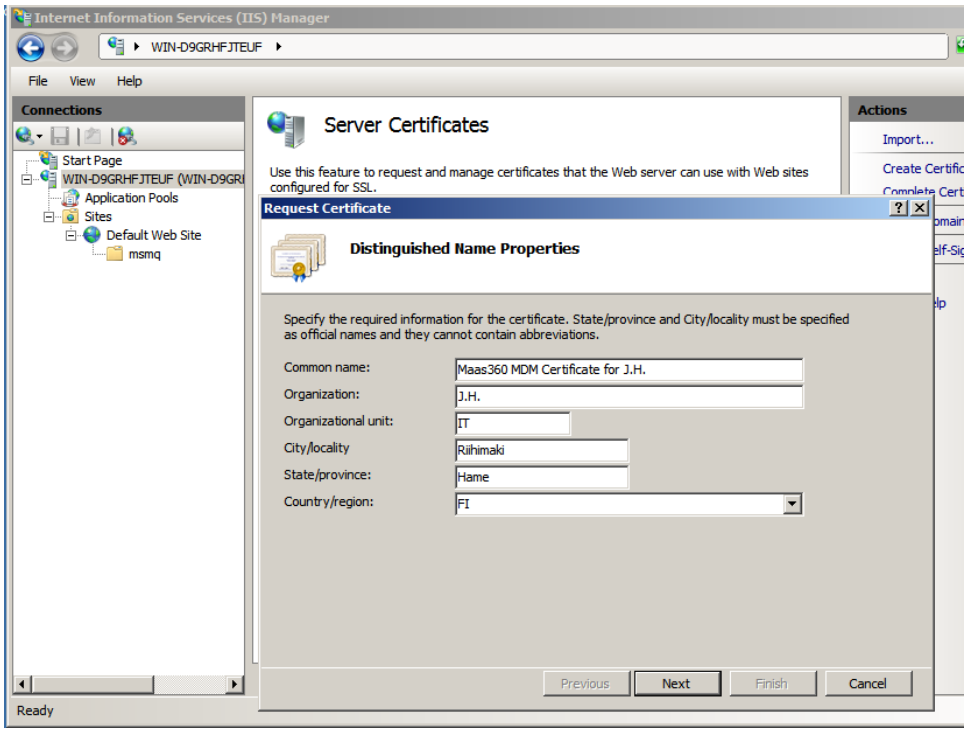
Kuva 14. Exchange ActiveSync – asetukset Maas360:ssa.

3.3 Käyttöönottotoimenpiteet

Käyttöönoton yhteydessä on tehtävä tarvittavat alkuasetukset. Tässä luvussa on selvitetty toimenpiteitä, jotka ovat pakollisia riippumatta keskitetyn hallintaohjelmiston valmistajasta. Tutkituista keskitetyn hallinnan ratkaisuista ainakin AirWatch ja Maas360 tarjoavat havainnollisia askel askeleelta – ohjeita tässä luvussa yleisesti käsiteltyihin toimenpiteisiin.

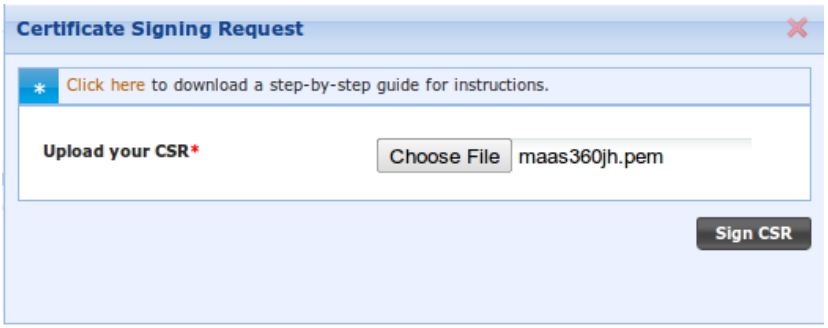
3.3.1 Apple Push Notification Service – sertifikaatin luominen

Hallintakäyttöliittymään kirjautumisen jälkeen pääkäyttäjän on ensimmäiseksi hankittava Apple MDM – sertifikaatti APNS:n käyttöön (ks. luku 2.1.1). Sen hankkimiseksi tarvitaan maksuton Apple ID – käyttäjätili. Sertifikaatin allekirjoituspyyntö (CSR) voidaan luoda Windows Serverillä (pääkäyttäjän oikeuksilla) tai Mac OS X – työaseman Keychain Access – työkalulla (Fiberlink Communications Corp 2012, 3-4). Operaation demonstroimiseksi tässä opinnäytetyössä luotiin virtuaalikoneelle Windows Server 2008R2 Enterprise – palvelin. Sertifikaatin myöntäjänä käytettiin itse tehtyä CA:ta (”OPNTESTCA”).



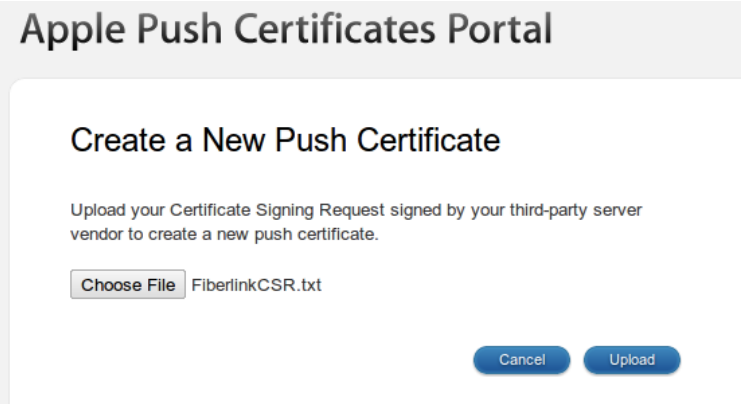
Kuva 15. CSR:n luominen Windows Server 2008R2:ssa.

Sertifikaatin luominen aloitetaan Internet Information Services Managerin Create Certificate Request – toiminnolla. Avainkoon (key bit length) tulee olla 2048 bittiä. Mikäli avainkoko on väärä, Apple Push Certificates Portal ei hyväksy sertifikaattipyyntöä. Luotu tiedosto (maas360jh.pem) tallennetaan palvelimen tiedostojärjestelmään (Kuva 15). Seuraavaksi tiedosto ladataan Maas360:n hallintakäyttöliittymään, jolloin se allekirjoitetaan digitaalisesti hallintaohjelmiston valmistajan toimesta (Kuva 16). Selaimen ladattavaksi palautetaan tiedosto FiberlinkCSR.txt.

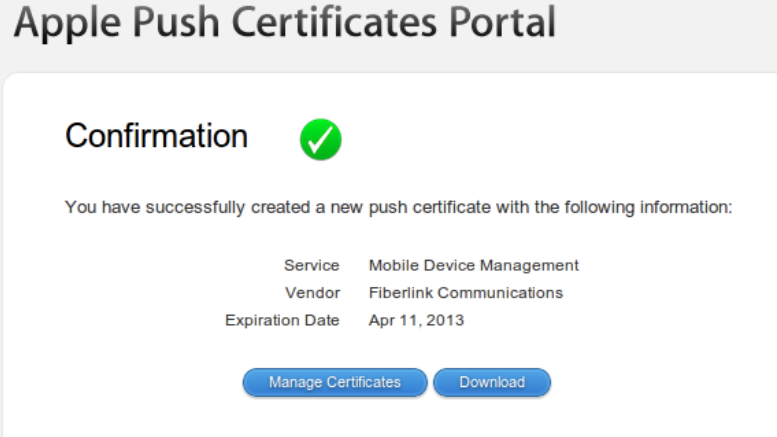


Kuva 16. Windows Server 2008R2:lla luodun CSR:n lataaminen.

Kirjautumalla osoitteeseen https://identity.apple.com/pushcert/ Apple ID – tunnuksella päästään syöttämään saatu FiberlinkCSR.txt – tiedosto Applen järjestelmään (Kuvat 17 ja 18).

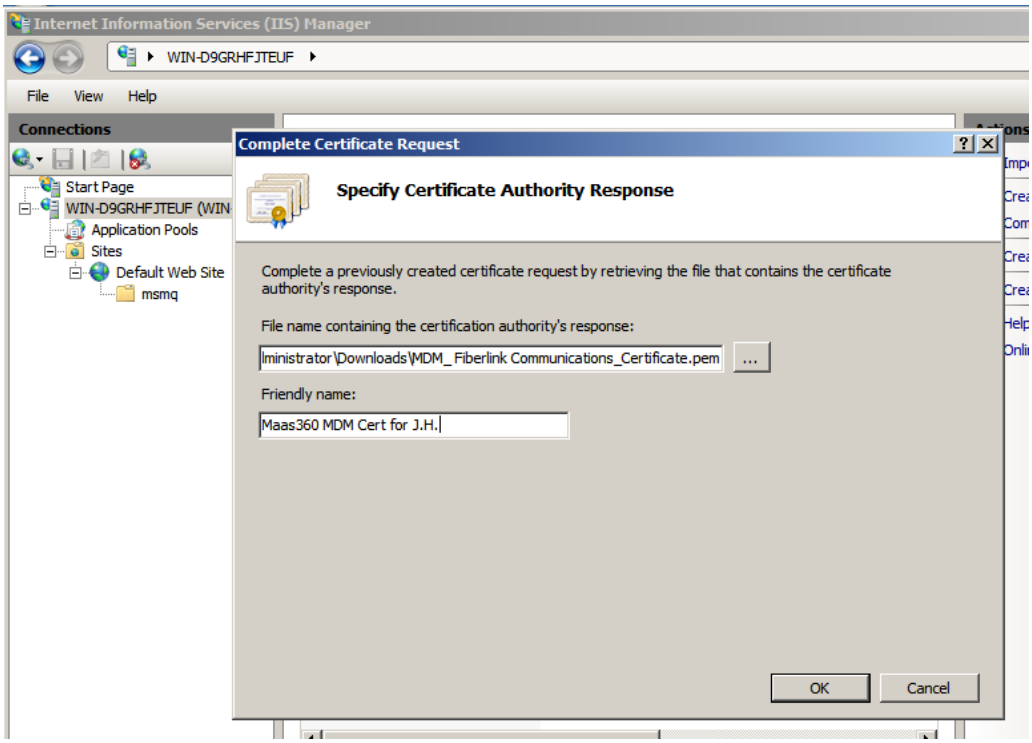


Kuva 17. Apple Push Certificates Portal – palvelu, vaihe 1.



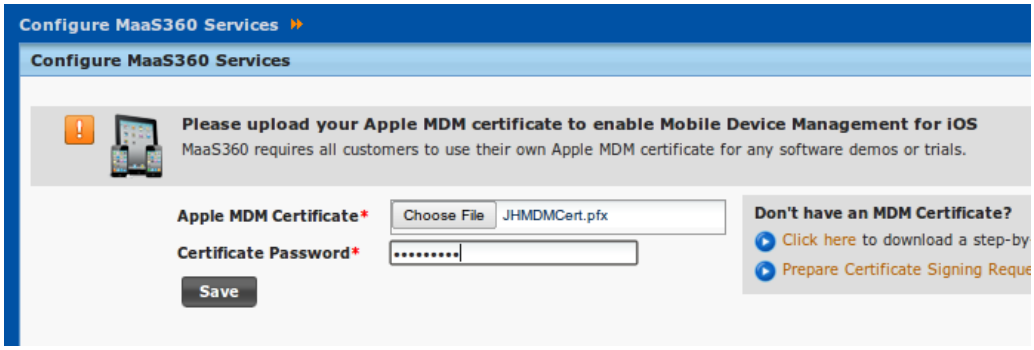
Kuva 18. Apple Push Certificates Portal – palvelu, vaihe 2.

Palvelusta saadaan ladattua selaimella jälleen uusi PEM – tiedosto (MDM_Fiberlink_Communications_Certificate.pem). Windows Serverissä käytetään Complete Certificate Request – toimintoa tälle tiedostolle (Kuva 19).



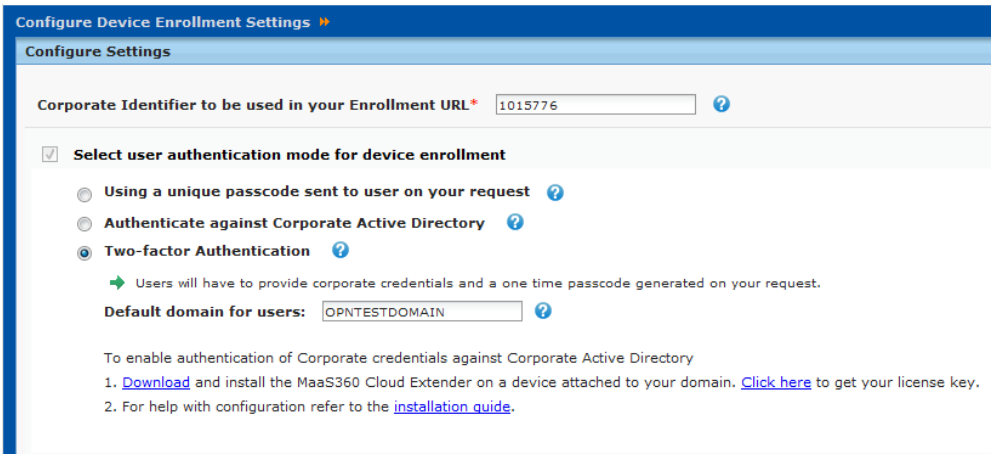
Kuva 19. CSR:n loppuunvienti Windows Server 2008R2:ssa.

Tämän jälkeen valmis sertifikaatti viedään PFX – tiedostomuotoon Export – toiminnolla, minkä yhteydessä määritetään tiedostolle myös salasana. PFX – tiedosto syötetään salasanoineen Maas360:n hallintakäyttöliittymään (Kuva 20), minkä jälkeen APNS on käytössä. Sertifikaatti on oletusarvoisesti voimassa vuoden kerrallaan. Sen uudistaminen tapahtuu edellä mainitussa Apple Push Certificates – palvelussa.



Kuva 20. Sertifikaatin lopullinen käyttöönotto Maas360:ssa.

3.3.2 Käyttäjien autentikointi



Kuva 21. Käyttäjien tunnistamisen asetukset Maas360:ssa.

Seuraava tärkeä valinta on mobiililaitteiden käyttäjien tunnistukseen käytettävä menetelmä. Koska käyttäjien määrä on yritysympäristössä useimmiten suuri, on hyödyllistä sitoa keskitetyn hallinnan piirissä olevat mobiililaitteet esimerkiksi työasemiin kirjautumiseen käytettäviin tunnuksiin. Esimerkkinä käytetty Maas360 tukee kolmea erityyppistä autentikointia (Kuva 21). Käyttäjältä voidaan vaatia yksinkertaista uniikkia avainlukua (passcode), tai tunnistautumista olemassa olevilla Active Directory – tunnuksilla. Kutsuna toimii hallintakäyttöliittymän kautta tekstiviestinä tai sähköpostina lähetetty URL – osoite, johon avainluku tai Active Directory – tunnukset syötetään. SaaS – palvelun yhdistäminen yrityksen lähiverkossa toimivaan Active Directory - toimialueeseen vaatii kuitenkin tukisovelluksen asentamista. Maas360:ssa tämä on toteutettu Cloud Extender – laajennusohjelmalla. Kolmas, kahden ensimmäisen yhdistelmään perustuva tunnistus on kaikkein tietoturvallisin vaihtoehto.

3.4 Tekniset rajoitukset

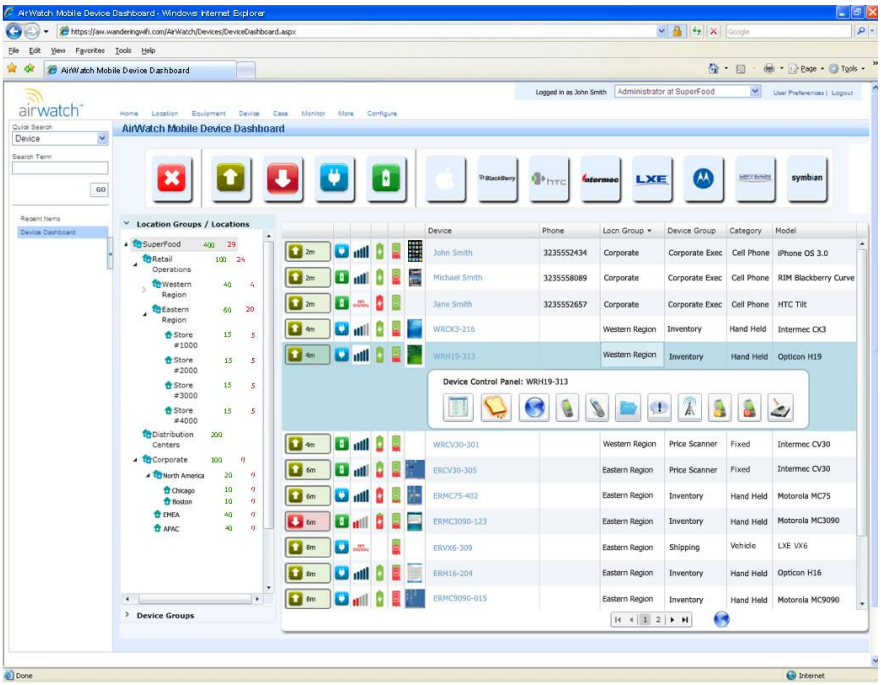
Opinnäytetyön vaatimuksissa mainituista toiminnoista (etätyhjennys, varmuuskopointi, yhteystietojen synkronointi, kloonaus) suurin osa on tuettuna Apple MDM:n ja OMA – DM:n standardissa. Sähköpostiasiakasohjelman (FirstClass Mobile) asentaminen iOS – ympäristöön keskitetyllä hallinnalla vaatii Applen asettamista rajoituksista johtuen lisäselvitystä. iOS – ympäristössä sovellusten asentaminen tapahtuu tavallisesti App Store – verkkokaupan välityksellä. Yrityskäytössä App Store voidaan kuitenkin poistaa mobiililaitteen käyttäjän näkyvistä etähallintapalvelimesta käsin, ja siirtyä ns. Managed apps – tilaan (Apple 2012, 5-6). Tällöin mobiililaitteen loppukäyttäjä ei voi itse asentaa uusia tai poistaa olemassaolevia sovelluksia puhelimeensa ilman etähallinnan pääkäyttäjän hyväksyntää. Managed – tilassa voidaan mobiililaitteisiin asentaa sekä kolmannen osapuolen julkisia että yrityksen omia sovelluksia (in-house apps). Maksullisen sovelluksen massakäyttöönotto vaatii Volume Purchasing Program (VPP) – lisenssikoodin syöttämistä etähallintaso-

vellukseen. Managed apps – tila on iOS:n version 5 myötä käyttöönotettu ominaisuus, ja sitä tukevat tutkituista etähallintaratkaisuista ainakin Capricode SyncShield, Maas360 ja AirWatch.

3.5 Vaihtoehdot

Liitteessä 1 listatuista etähallintaohjelmistoista päädyttiin valitsemaan tarkempaan tarkasteluun kolme kappaletta. Valinnan perusteena olivat ohjelmistojen ajantasaisuus, ominaisuudet, dokumentaatio ja toimeksiantajan vaatimuksien täyttäminen.

3.5.1 AirWatch Mobile Device Management

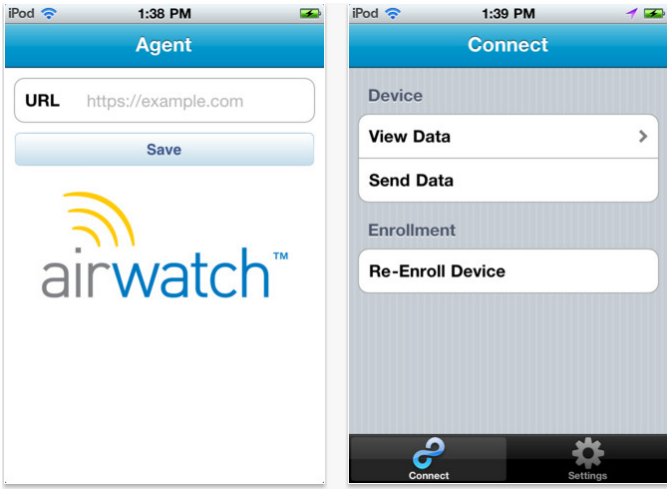


Kuva 22. Kuvakaappaus AirWatch – ohjelmiston hallintakäyttöliittymästä.

AirWatch MDM on Yhdysvaltalaisen AirWatch LLC.:n kehittämä keskitetyn hallinnan ohjelmisto. Yritys on tarjonnut mobiilipalveluita vuodesta 2003, erikoistuen yritysympäristöihin. Muita yrityksen palveluita ovat erilaiset SaaS – pohjaiset sähköposti-, sovellus- ja sisällönhallintajärjestelmät. AirWatch MDM tukee kaikkia yleisimpiä mobiilialustoja (Liite 1). Hallintakäyttöliittymä on HTML5 – tekniikkaan pohjautuva. Perusominaisuuksien lisäksi AirWatch MDM sisältää yritysverkon hallinnoinnin kannalta hyödyllisiä lisäosia. Käyttäjien tunnistautumiseen voidaan käyttää olemassa olevaa Active Directory – tai LDAP – hakemistopalvelua, joskin näiden palveluiden hyödyntäminen SaaS – palvelun kautta vaatii erillisen laajennuksen (ks. luku 3.3.2). SEG (Secure Email Gateway) – järjestelmällä voidaan valvoa ja raportoida poikkeuksia käyttäjien sähköpostikäyttäytymisessä. Mobiililaitekannasta ja käyttäji-

en aktiviteeteistä voidaan koostaa raportteja, joita voidaan käyttää palveluiden jatkokehittämiseen ja vianetsintään. Ohjelmiston käyttöönotto – ohjeet ja muu dokumentaatio on saatavilla valmistajan WWW – sivuilta PDF – muodossa. AirWatch LLC. tarjoaa myös WWW – pohjaisia koulutuspalveluita ja käyttöönottoa edeltävää suunnittelukonsultointia. Käytönaikaista ohjeistusta ei opinnäytetyön tutkimustyön ohessa ollut mahdollisuutta testata. Kuten useimmissa muissakin tarkastelluissa ohjelmistoissa, AirWatch MDM:n SaaS – versiosta on saatavilla 30 päivän ilmainen kokeiluversio.

AirWatch MDM:n Agent – sovelluksen avulla pääkäyttäjä voi suorittaa ylläpitotoimenpiteitä etäkäytöllä. Sovellus on myös mobiililaitteen loppukäyttäjän apuna keskitetyn hallinnan piiriin liittyessä (Kuva 23).



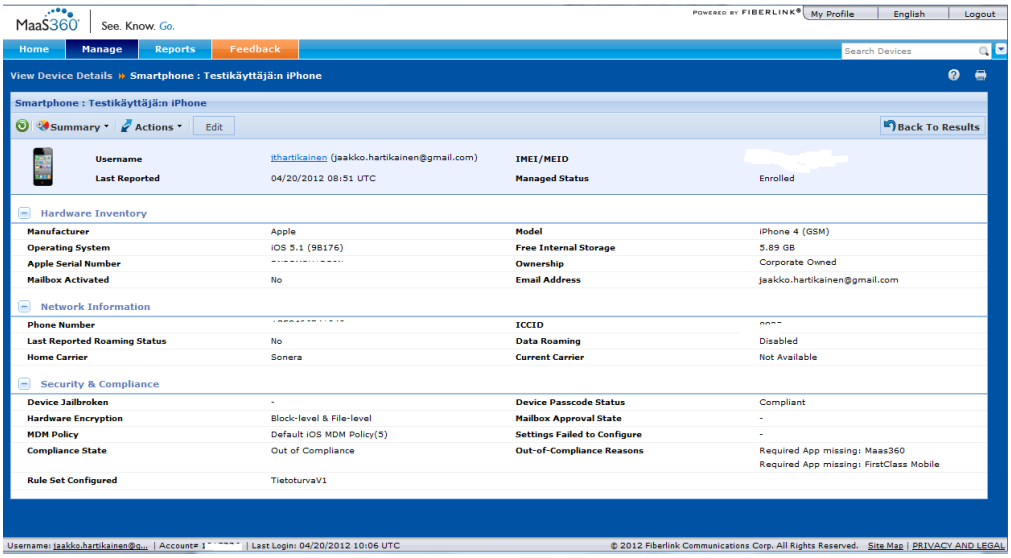
Kuva 23. AirWatch MDM:n Agent – sovellus iOS – laitteille.

3.5.2 Capricode SyncShield

Capricode SyncShield on opinnäytetyön kirjoitushetkellä ainoa suomalainen MDM – ohjelmisto. SyncShield – ohjelmiston lisäksi yritys tarjoaa jälleenmyyjien kautta (mm. Sonera) etäkoulutusta ja tukea tuotteilleen muun muassa Cisco WebExillä (Onnela, sähköpostiviesti 2.4.2012). SyncShieldiä on saatavilla pääasiassa kahtena eri SaaS - vaihtoehtona, peruspalveluna (standard) – ja hallittuna (managed). Jälkimmäisessä auktorisoidun jälleenmyyjän henkilökunta vastaa järjestelmän konfiguroinnista ja hallinnasta asiakkaan toiveiden mukaan. Managed – vaihtoehdon kertamaksu on kuitenkin kalliimpi (ks. Liite 1). SyncShield tukee muiden vaihtoehtojen tavoin kaikkia yleisimpiä mobiilialustoja (Liite 1). Agent - sovellus on saatavilla iOS:lle (Kuva 24), Androidille ja Symbianille.

Kuva 24. CapriCode SyncShield:n Agent – sovellus App Storessa.

3.5.3 Maas360



Kuva 25. Ruutukaappaus Maas360 – ohjelmistosta.

Maas360 on yhdysvaltalaisen Fiberlink Communications, Inc.:n valmistama keskitetyn hallinnan ohjelmisto. Se on tarkastelluista vaihtoehdoista ainoa, jota tarjotaan ainoastaan SaaS – ratkaisuna. Tuettuna ovat käytännössä kaikki mobiilialustat, mukaan lukien harvinaisempi WebOS (Liite 1). Hallintakäyttöliittymä on HTML5 – pohjainen. Maas360:n kokeiluversioon liitettiin opinnäytetyön työnantajalta lainattu iPhone 4 – puhelin perustoimintojen ja tietoturvaseikkojen kokeilemiseksi. Käyttöliittymän perustoimivuudessa havaittiin puutteita Firefox – ja Google Chrome – selaimilla, koska näennäisestä alustariippumattomuudesta huolimatta käyttöliittymä on teknisesti optimoitu Microsoft Internet Explorerille. Mainittakoon, että Maas360 valittiin vuonna 2012

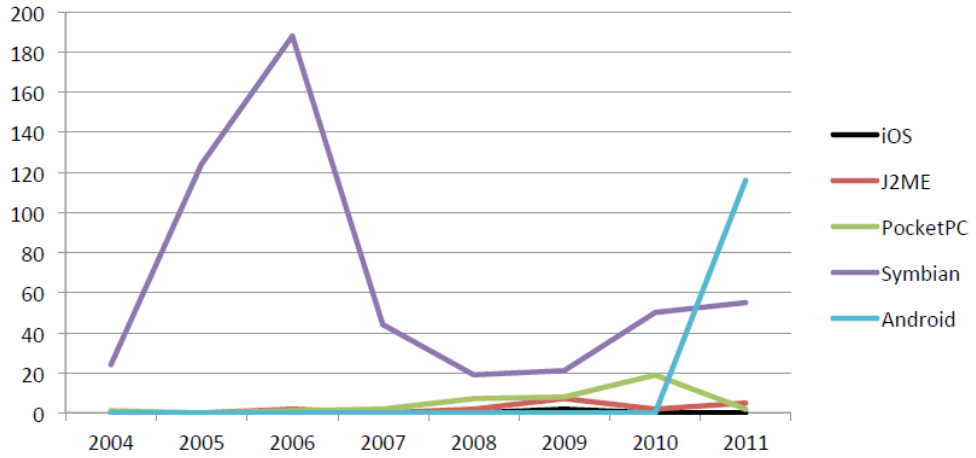
Mobile World Congress – tapahtuman parhaimmaksi mobiilijärjestelmiin keskittyneeksi yritystuotteeksi riippumattoman tuomariston toimesta.

4 TIETOTURVAONGELMAT

4.1 Ongelmat ja uhkatekijät

Apple iOS – ja Symbian – laitteiden suorituskyvyn ja ominaisuuksien lisääntyminen pakottaa käsittelemään niiden tietoturvaa samoin periaattein kuin varsinaisten kannettavien tietokoneidenkin. Yritysympäristössä usein käytettyjä tekniikoita, kuten laitteistopohjaista käyttöjärjestelmän ja massamuistin salausta ei voida toteuttaa aukottomasti mobiililaitteilla uhraamatta käyttäjäystävällisyyttä. Tällöin mobiililaitteen kadotessa fyysisesti omistajaltaan voidaan siitä poimia arkaluontoista tietoa, jota voidaan käyttää vaikkapa kohdistetun verkkohyökkäyksen suunnitteluun. iOS – käyttöjärjestelmä on versiosta 4 lähtien käyttänyt Data Protection – ominaisuutta sähköpostivälimuistin ja salasanojen suojaamiseen (Apple Inc 2011, 1). Opinnäytetyön tutkimustyön aikana havaittiin kuitenkin, että salausjärjestelmä on murrettu toistuvasti kolmannen osapuolen toimesta ohjelmistopohjaisilla hyökkäyksillä (Zdziarski 2012, 1-3). Symbian – ympäristössä vastaavaa salausjärjestelmää ei ole saatavilla lainkaan.

Eräs iOS – sekä Android – laitteiden yritystietoturvaa olennaisesti heikentävä tekijä on ns. murtaminen (jailbreaking/rooting). Murtaminen tarkoittaa laitevalmistajan virallisen ohjelmiston rajoituksien kiertämistä ja mobiililaitteen oman pääkäyttäjän (root) oikeuksien antamista niitä haluaville sovelluksille. Se poistaa myös käytöstä digitaalisten allekirjoitusten varmistuksen (code signing). Loppukäyttäjä pyrkii murtamisella asentamaan mobiililaitteeseen kolmannen osapuolen sovelluksia, jotka tarvitsevat poikkeuksellisia käyttöoikeuksia. Tämä toimenpide altistaa iOS – laitteen tietoturvariskeille, sillä käyttöjärjestelmä sallii tuntemattomasta lähteestä peräisin olevien, allekirjoittamattomien sovelluksien asentamisen. Laitevalmistaja Apple pyrki aikaisemmin estämään murtamisen aktiivisesti, mutta Yhdysvalloissa pätevän DMCA – lain muutoksien takia estotoimenpiteistä on jouduttu osittain luopumaan (U.S. Copyright Office 2012). Mobiililaitteille suunnattuja haittaohjelmia tutkineet yritykset, kuten Fortinet, toteavat kuitenkin että yli 50% kaikista tutkituista haittaohjelmista on suunnattu Symbianille (Fortinet 2011; F-Secure 2011, 14) (Kuva 26).



Kuva 26. Kaavio haittaohjelmien määrän kehityksestä eri mobiilialustoilla (F-Secure 2011, 14).

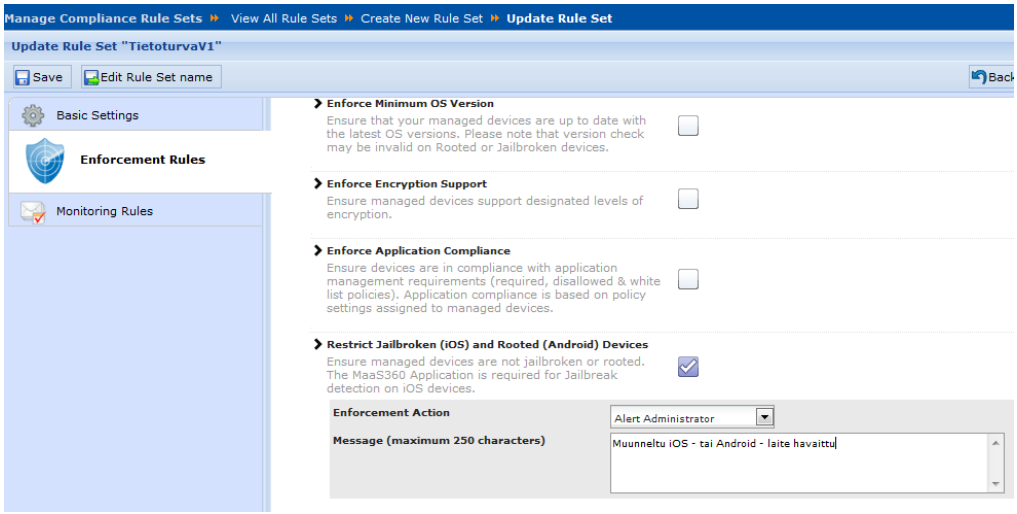
Yritystyöasemiin virustorjunta- ja palomuuriohjelmistoja valmistavat yritykset, kuten F–Secure, Symantec ja Kaspersky tarjoavat mobiililaitteisiin asennettavia ohjelmistoja haittaohjelmien torjuntaan. Näiden käyttöönotto ei ole kuitenkaan yleistynyt yrityksissä lisääntyneestä mobiiliturvallisuuden kustannuksista huolimatta (Symantec 2012, 4-6). Opinnäytetyön tutkimustyön aikana etsittiin aktiivisesti mahdollisia tietoturva – aukkoja. CERT-FI – tietoturvaorganisaation ja National Vulnerability Databasen hakutoiminnolla ei löydetty kolmea tarkasteltua ohjelmistoa (Capricode SyncShield, AirWatch, Maas360) koskevia avoimia haavoittuvuuksia.

Muita toimeksiantajan tietoturvan kannalta merkittäviä seikkoja ovat mm. Applen käyttöön ottama iCloud – pilvipalvelu. iCloud on yksityisille käyttäjille suunnattu palvelu, johon voidaan varmuuskopioida käyttäjän kaikkien iOS – mobiililaitteiden sisältämät tiedot. Pilvipalveluun kirjaudutaan Apple ID – tunnuksilla. Tietoturvariskin muodostaa tilanne, jossa yrityksen sisäistä dataa (sähköpostit, muut dokumentit) säilötään iCloud – palveluun. Mikäli mobiililaite varastetaan tai katoaa omistajaltaan, voi tuntematon osapuoli päästä käsiksi entisen käyttäjän tallentamiin tietoihin. Useimmat keskitetyn hallinnan ohjelmistot tarjoavat kuitenkin mahdollisuuden iCloud – varmuuskopioinnin pakottamiseen pois käytöstä.

SaaS – ratkaisuna toimitettujen palveluiden tietoturvataso on yrityskäytössä vähintäänkin riittävä. Pääkäyttäjä tunnistautuu käyttäjätunnuksella ja salasanalla, jonka tulisi olla riittävän monimutkainen ja pitkä. Suurimmaksi uhaksi jää käytännössä fyysinen tai ohjelmistopohjainen murtautuminen palveluntarjoajan laitesaleihin.

4.2 Suojatoimenpiteet

Yritysympäristössä keskitetyn mobiililaitteiden hallinnan käyttöönotto vähentää tietoturvariskejä tuntuvasti jo itsessään. Toimeksiantajan lähtötilanteessa jokaiselle mobiililaitteelle voidaan asettaa yrityksen käytännön mukaiset tietoturva – asetukset, mutta niiden muuttaminen ja tietoturvapoliitikan noudattamisen valvominen jälkeenpäin ei ole mahdollista ilman aikaa vievää käsin konfigurointia. Tällöin ei voida myöskään reagoida riittävän nopeasti mahdollisiin uusin tietoturvahyökkäyksiin. Keskitettyä hallintaa käyttämällä varmistetaan, että kaikissa hallinnan piirissä olevissa mobiililaitteissa on vaikkapa käytössä viimeisin versio laitevalmistajan virallisesta ohjelmistosta. Opinnäytetyössä tutkituista hallintaohjelmistoista ainakin AirWatch ja Maas360 kykenevät suorittamaan uusille laitteille automatisoidusti tietoturvakyselyjä (audit, compliance report). Pääkäyttäjää varoitetaan mahdollisista poikkeavuuksista ja puutteista. Luvussa 4.1 mainittu laitteen murtaminen voidaan havaita ja/tai estää Maas360 – ohjelmistossa (Kuva 27). Ominaisuus vaatii kuitenkin, että Maas360:n agent – sovellus on asennettu mobiililaitteeseen.



Kuva 27. Murtamisen havaitseminen Maas360:ssa.

Luvussa 4.1 niinikään mainittu iCloud – pilvipalvelu on syytä poistaa käytöstä kokonaan. Suositeltavaa on myös, että App Store – sovelluskauppa vaihdetaan käyttäjien vapaasti käytössä olevasta tilasta Managed Apps – tilaan. Tällöin pääkäyttäjän on hyväksyttävä toimeksiantajan mobiililaitteisiin asennettavat lisäsovellukset. Opinnäytetyön toimeksiantajan mobiililaitteisiin oli lähtötilanteessa otettu käyttöön operaattorin tietoihin perustuva paikannus tarvittaessa fyysisten uhkien varalta. Tätä voidaan parantaa edelleen ottamalla käyttöön mobiililaitteen GPS – seuranta, joka kirjaa ylös mobiililaitteen viimeisimmän tiedetyn sijainnin vaikkapa 6 tunnin välein. Toiminto lisää päivitystiheydestä riippuen akun kulutusta, mikä saattaa taas vaikuttaa käyttäjien työtehoon.

5 TULOKSET

5.1 Kuvaus tutkimustyön toteutuksesta

Opinnäytetyön pääasiallinen tutkimustyö suoritettiin tammikuun ja huhtikuun 2012 välisenä aikana. Pääasiallisena tietolähteenä käytettiin laite- ja ohjelmistovalmistajien, kuten Applen, Nokian ja Microsoftin teknistä dokumentaatiota, käyttöohjeita, esitteitä, koulutusvideoita ja muita artikkeleita. Erilaisten kaavioiden, taulukoiden ja valmiiden selvityksien selaamiseen ja vertailuun käytettiin Google – hakukonetta. Lisätietoja eri ohjelmistojen hinnoittelusta ja muista tiedoista selviteltiin sähköpostitse. Mobiilijärjestelmien erittäin nopean kehityksen takia kirjallisuutta käytettiin rajallisesti. Käytännön seikkoja pyrittiin kokeilemaan käyttämällä toimeksiantajalta lainattua iPhone 4 – puhelinta sekä kokeiluversiona saatavilla ollutta Maas360 – ohjelmistoa. Opinnäytetyössä hyödynnettiin myös Windows Server 2008R2 Enterprise – käyttöjärjestelmää virtuaaliympäristössä. Käytännön teknistä koekäyttöä pystyttiin suorittamaan vain Maas360 - ohjelmiston kokeiluversiolla. Muiden valmistajien kohdalla kokeiluversioiden käyttöoikeuden hankkimiseksi olisi tarvittu toimeksiantajan tietojen luovuttamista eteenpäin.

Tutkimustyötä varten oli myös suunnitelmana teettää pienimuotoinen WWW – pohjainen kysely tai haastattelu henkilöstön mobiililaitteiden käyttötottumuksista ja tietoturvakäytäntöjen noudattamisesta. Kyselyä ei kuitenkaan toteutettu toimeksiantajan edustajan huomautettua että työntekijöiden aikaa ei siihen ole mahdollista käyttää. Kysely korvattiin tutkimalla valmiiksi julkaistuja vastaavia aineistoja.

Tutkimustyön tuloksista koostettiin Excel – taulukko (Liite 1). Tähän taulukkoon on listattu suurimmat keskitetyn hallinnan ohjelmistojen valmistajat päätuotteineen, tuotteen tukemat mobiilialustat sekä tiedot siitä, onko tuotetta saatavilla pilvipalveluna ja mitkä ovat teoreettiset käyttöönoton kiinteät kustannukset. Taulukosta karsittiin pois opinnäytetyön vaatimuksia täyttämättömät ohjelmistot (ks. luku 2.3, 3.1), sekä ne ohjelmistot joita ei ollut saatavilla pilvipalveluna.

5.2 Havaintoja tutkimustyön pohjalta

Mobiililaitteiden keskitettyyn hallintaan tarkoitettujen ohjelmistojen valmistajien kirjo on laaja. Suuret laitteistovalmistajat määrittelevät keskitetyn hallinnan vähimmäisvaatimukset ja teknisen toteutuksen, mutta eivät tarjoa itse valmiita ohjelmistoja. Kolmannen osapuolen keskitetyn hallinnan järjestelmien valmistajissa on mukana suuria ohjelmistoyrityksiä kuten HP ja Symantec, sekä yksittäisiä toimijoita, kuten Fiberlink Communications ja suomalainen

Capricode. Nopeasti markkinoiden muutoksiin mukautuvat ja uusien mobiilialustojen tukemiseen kykenevät yhden palvelun ympärille perustuvat yritykset kykenevät tarjoamaan selvästi kattavampia palveluita. Pilvipalveluiden hyödyntäminen tulee muuttumaan lähitulevaisuudessa yrityksille edukkaimmaksi vaihtoehdoksi alhaisten käyttöönottokustannusten ja helpon ulkoistamismahdollisuuden takia. Vaikka laitteet sijaitsevat fyysisesti muualla kuin yrityksen omissa laitetiloissa, onnistuu yhdistämisen olemassa olevaan infrastruktuuriin, esimerkiksi Active Directory – tai LDAP – hakemistopalveluihin erilaisilla asiakkaan verkkoon liitettävillä lisäohjelmistoilla.

Opinnäytetyön toimeksiantajan, Suomen Lehtiyhtymä Oy:n vaatimukset keskitetyn hallinnan suhteen pystytään toteuttamaan saatavilla olevilla valmiilla ratkaisuilla ilman ylimääräistä kehitystyötä tai kalliin ohjelmistokonsultoinnin tarvetta. Toimeksiantajan edustajan kanssa käytyjen keskustelujen perusteella on tärkeää, että käyttöön ennen pitkää otettava keskitetyn hallinnan ohjelmisto voidaan hankkia ulkoistetun ylläpidon kera.

Mobiililaitteiden keskitetyllä hallinnalla saavutetaan kiistaton tietoturvaetu, sillä toimeksiantajan mobiililaitteita uhkaavat todennäköisimmät tietoturvariskit liittyvät puutteellisiin asetuksiin ja älypuhelimien kykyyn ajaa ei – toivottuja sovelluksia. Apple iPhone ja iPad – laitteiden tietoturvaominaisuudet ovat huomattavasti vanhempaa Symbian - käyttöjärjestelmää käyttäviä laitteita vahvemmat. Pelkästään Symbian – käyttöjärjestelmälle suunnattujen haittaohjelmien määrän takia on suositeltavaa että Nokian E7 ja C7 – laitteet korvattaisiin esimerkiksi Windows Phone 7.5 - käyttöjärjestelmään perustuvilla laitteilla.

5.3 Johtopäätökset

Opinnäytetyön ensisijaisena tavoitteena oli selvittää toimeksiantajan tarkoituksiin sopivat keskitetyn hallinnan ohjelmistot sekä suositella näistä tutkimustyön perusteella sopivinta. Myös mobiililaitteiden tietoturvaan liittyvät kehitysehdotukset tuodaan esille. Lopullisen vertailun ja tarkastelun kohteeksi päätyivät AirWatch, Capricode SyncShield ja Fiberlink Maas360. Kuten liitteen 1 taulukosta voidaan päätellä, kaikki kolme ovat ajan tasalla tuettujen mobiilialustojen suhteen. AirWatch jätettiin vertailusta kuitenkin pois, sillä sen Symbian – käyttöjärjestelmän tuessa oli ongelmia tutkimustyön perusteella. CapriCode SyncShieldin varsinaista käyttöliittymää ei ollut mahdollisuutta kokeilla käytännössä opinnäytetyön tutkimustyön aikana, mutta sen valintaa puolsi muun muassa toimeksiantajan toive siitä, että palvelu olisi mahdollista käyttöönottaa mahdollisimman ulkoistettuna. SyncShield oli tuotteista ainoa, jolla oli suomalainen jälleenmyyjä, Sonera Oy.

Fiberlink Maas360 – tuotteen käyttöliittymä havaittiin intuitiiviseksi ja helpoksi käyttää. Luvussa 3.3 kuvatut käyttöönottotoimenpiteet onnistuivat on-

gelmitta tutkimustyön aikana. Hallintakäyttöliittymän toimivuudessa oli ongelmia tietyillä WWW – selaimilla, toiminta oli varminta Internet Explorerilla. Koekäyttöä varten keskitettyyn hallintaan liitetyn iPhone 4 – puhelimen hallinnassa esiintyi ajoittaisia viiveitä. Tärkeimmät toiminnot saatiin kuitenkin testattua, ja Maas360:aa suositellaan siten toissijaisena vaihtoehtona toimeksiantajan käyttöön.

Tietoturvan näkökulmasta suurimmat haasteet ovat tyypilliset fyysiset riskit, iOS – laitteiden murtaminen (jailbreaking), iCloud – pilvipalvelun riskit sekä Symbian - käyttöjärjestelmän vanhentuneesta arkkitehtuurista johtuvat haavoittuvuudet. Näistä kolmeen ensin mainittuun voidaan puuttua riittävän tiukoilla tietoturvakäytännöillä, jotka asetetaan keskitetysti. Havaittiin, että iOS – mobiililaitteiden laitteistopohjainen Data Protection – salausmenetelmä tarjoaa keskinkertaista suojaa fyysisiltä riskeiltä. Järjestelmä on kuitenkin murrettu ohjelmistopohjaisilla hyökkäyksillä. Puhelimen kadotessa olemassa olevaa operaattoripohjaista paikannusta voidaan tarkentaa mobiililaitteen omia GPS – tietoja käyttämällä. Symbian – käyttöjärjestelmän haittaohjelmatilanteen ja OMA – DM – protokollan iän takia suositellaan mahdollisimman nopeaa migraatiota esimerkiksi uudempiin Windows Phone 7.5 – laitteisiin.

LÄHTEET

Apple Inc. 2011. iOS: Understanding Data Protection. Viitattu 17.4.2012. http://support.apple.com/kb/HT4175

Apple Inc. 2012. Enterprise Deployment Guide For iOS Devices. Viitattu 17.2.2012. http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf

Apple Inc. 2012. iPhone In Business – Integration – Mobile Device Management in iOS. Viitattu 17.2.2012. http://www.apple.com/iphone/business/integration/mdm/

Apple Inc. 2011. Deploying iPhone and iPad Overview. Viitattu 24.2.2012. http://images.apple.com/ipad/business/docs/iOS_MDM.pdf

Cellstrat.com. 2012. Maas360 Won Best Enterprise Mobile Services @ MWC 2012. Viitattu 20.4.2012. http://www.cellstrat.com/blog/?p=2138

Chacko, C. 2007. OTA - DM (Over the Air Device Management). Viitattu 2.4.2012. http://wireless.ittoolbox.com/research/otadm-over-the-air-device-management-3472

Cisco Systems. 1998. White Paper: Cisco System's Simple Certificate Enrollment Protocol. Viitattu 12.3.2012. http://www.cisco.com/warp/public/cc/pd/sqsw/tech/scep_wp.pdf

Edge, C. 2010. Enterprise iPhone and iPad Administrator's Guide. Berkeley: Apress Academic.

F-Secure. 2011. Mobile Threat Report, Q4 2011. Viitattu 17.4.2012. http://www.f-secure.com/weblog/archives/Mobile_Threat_Report_Q4_2011.pdf

Fiberlink Communications Corp. 2012. Generating an APNs Certificate. Viitattu 11.4.2012. http://content.maas360.com/www/support/mdm/assets/APNs_Cert_Guide.pdf

Fortinet. 2011. Mobile Malware Statistics. Viitattu 17.4.2012. http://blog.fortinet.com/mobile-malware-statistics/

Faas, R. 2010. Mobile IT Guide to iPhone Deployment and Management with Apple's iOS 4. Viitattu 17.2.2012. http://www.enterprisemobiletoday.com/features/management/article.php/3897471/Mobile-IT-Guide-to-iPhone-Deployment-and-Management-with-Apples-iOS-4.htm

Gartner Inc. 2012. Worldwide Smartphone Sales to End Users by Operating System in 4Q11. Viitattu 3.4.2012.
http://www.gartner.com/it/page.jsp?id=1924314

Jipping, M. 2002. Symbian OS Communications Programming. West Sussex: John Wiley & Sons. Ltd.

Suomen Lehtiyhtymä Oy. 2012. Konserni. Viitattu 17.2.2012. http://www.lehtiyhtyma.fi/yritys.html

Microsoft, 2006. Software as Service (SaaS): An Enterprise Perspective. Viitattu 2.4.2012.
http://msdn.microsoft.com/en-us/library/aa905332.aspx

Microsoft. 2010. AD CS: Network Device Enrollment Service. Viitattu 29.3.2012.
http://technet.microsoft.com/en-us/library/cc753784%28v=ws.10%29.aspx

Nieminen, T. 15.12.2011. Re: Lisätietoja opinnäytetyöstä. Vastaanottaja Jaakko Hartikainen. [Sähköpostiviesti]. Viitattu 17.2.2012.

Nokia Europe. Nokia for Business – Symbian Device Management. Viitattu 17.2.2012.
http://europe.nokia.com/find-products/nokia-for-business/device-management

Onnela, J. 2.4.2012. Re: Capricode SyncShield – tiedustelu. Vastaanottaja Jaakko Hartikainen. [Sähköpostiviesti]. Viitattu 11.4.2012.

Open Mobile Alliance. 2012. Technical Information - Publicly Available Documents. Viitattu 17.2.2012.
http://www.openmobilealliance.org/Technical/PublicMaterial.aspx

Phifer, L. 2011. Review: AirWatch Enterprise MDM for Apple iOS4.
http://www.esecurityplanet.com/views/article.php/3919161/Review-AirWatch-Enterprise-MDM-for-Apple-iOS4.htm

Symantec. 2012. State of Mobility Global Key Findings. Viitattu 17.4.2012.
http://www.slideshare.net/symantec/2012-state-of-mobile-survey-global-key-findings

U.S. Copyright Office. 2012. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies. Viitattu 17.4.2012.
http://www.copyright.gov/1201/

Zdziarski, J. 2012. Preventing Widespread Automated Attacks in iOS, Part 1. Viitattu 17.4.2012.
https://viaforensics.com/iphone-forensics/preventing-widespread-ios-application-infection.html

Liite 1

Vertailutaulukko keskitetyn hallinnan ohjelmistoista

ohjelmistot_versio2.xlsx

Sovelluksen nimi	Versio	Palvelinalusta	Tuetut m. käyt.	Työasemasovellus	SaaS	Agent	Hinnoittelu (SaaS)	Hinnoittelu(on-premise)	Hinnoittelu (appliance)
Capricode SyncShield	3.8.3	Windows Server 2008R2	iOS, Android, WP7, WM, Symbian, SE UIQ 2 & 3	ei	kyllä	kyllä	4-6,5€ per laite/kk + 500€ (**)		
AirWatch	5.17.1.3	Windows Server 2008R2	iOS, Android, WP7, WM, Symbian, BlackBerry	Windows	kyllä	kyllä	2,25€ per laite/kk + 1500€	30€ per laite/kk + 1500€ + 20% tuki	4880€ + 1500€ (*)
Fiberlink Maas360	2012	Windows Server 2008R2	iOS, Android, WP7, WM, Symbian, BlackBerry, WebOS	Windows, Mac	kyllä	kyllä			
MobileIron	N/A	Windows Server 2008R2	iOS, Android, WP7, Symbian, Blackberry, WebOS	ei	ei	kyllä	$4 per laite/kk, $75 pysyvä/laite		
McAfee Enterprise Mobility Management	10.1	Windows Server 2008R2	iOS, WP7, Android, BlackBerry	kyllä	ei	ei			
HP Mobile Management	3.10	Unix (Sun Solaris, Redhat Linux)	Vain OMA - DM - pohjaiset	ei	ei	ei			
Symantec Mobile Management	7.1	Windows Server 2003/2008R2	iOS, Android, WP7, WM, Symbian, BlackBerry	ei	ei	ei			
Zenprise Mobile Management	N/A	Windows Server 2008R2	iOS, Android, WP7, WM, Symbian, BlackBerry	Windows	kyllä	kyllä			
LANDesk Mobility Manager	9	Windows Server 2008R2	iOS, Android, WP7, Palm OS, Blackberry	ei	kyllä	ei			
Sybase Afaria MDM	7.6	Windows Server 2008R2	iOS, Android, (WP7?), WM, BlackBerry, Symbian	ei	ei (***)	ei			
MobiDM	N/A	Windows Server 2008R2	iOS, Android, WP7, WM, Symbian, Blackberry	ei	kyllä	kyllä			

*) sisältää 50 kpl ns. Perpetual License (pysyvä lisenssi)
**) standard - lähtöhinta, managed: alk. 1000€
***) "Relay server" - ratkaisulla