Opinnäytetyö (AMK)

Tietotekniikka

Hyvinvointiteknologia

2015

Joonas Korgan

ÄLYPUHELIMIEN HALLINTA SOTI MOBICONTROL MDM -TUOTETTA KÄYTTÄEN

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietotekniikka | Hyvinvointiteknologia

2015 | 36

Juha Nikkanen | Mika Ventovuori

Joonas Korgan

ÄLYPUHELIMIEN HALLINTA SOTI MOBICONTROL MDM-TUOTETTA KÄYTTÄEN

SOTI MobiControl on SOTI:n tarjoama Mobile Device Management-ratkaisu, jonka avulla hallinnoidaan puhelimia, tabletteja sekä tietokoneita. Tämän opinnäytetyön tehtävänä oli asentaa ja käyttöönottaa Medbit Oy:lle SOTI MobiControl. Tarve MDM-ratkaisulle on, sillä suurin osa työntekijöistä käyttää yhä enemmän omia henkilökohtaisia älypuhelimiaan työn tekemiseen.

Yleistyneen Bring Your Own Device -käytännön lisäännyttyä yritysten tiedot ovat yhä useammin työntekijöiden omissa älypuhelimissa. Tämän vuoksi yritysten tiedot voivat päätyä vääriin käsiin helposti näin luoden tietoturvauhan yritykselle. On välttämätöntä, että yritykset varautuvat näihin riskeihin.

Työssä käsiteltiin, miten ja millä keinoilla luodaan turvallinen verkkoympäristö sekä miten MobiControl asennetaan Windows-palvelinympäristöön. Työssä luotiin turvattuja ja salattuja yhteyksiä älypuhelimien ja tuotantopalvelimen välillä HTTPS- ja LDAP-protokollia käyttämällä.

Tuloksena syntyneessä kokonaisuudessa SOTI MobiControllia käytetään jo useassa yrityksen laitteessa. Tällä hetkellä kuitenkin Medbit etsii myös muita MDM-ratkaisuja erityisesti Citrix-tuoteperheestä, sillä suurin osa Medbitin asiakkaista käyttää Citrixin tarjoamia sovelluksia.

ASIASANAT:

SOTI, MDM, AD, DA, HTTPS, Android, Windows, MobiControl, LDAP, IP, portti

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information Technology | Healthcare informatics

2015 | 36

Juha Nikkanen | Mika Ventovuori

Joonas Korgan

MANAGEMENT OF SMARTPHONES WITH SOTI MOBICONTROL

The aim of this thesis was to install and implement SOTI MobiControl, a new Mobile Device Management solution capable of managing phones, tablets and computers for Medbit Ltd. Medbit Ltd specializes in providing ICT-services for hospitals in the Southwestern Finland and Satakunta areas. As more and more personal smartphones are used by the employees, the need for a Mobile Device Management solution rose.

As the Bring Your Own Device policy is becoming more popular in the corporate world, it also brings in significant security risks. It allows the possibility for corporate data to end up in the wrong hands. To negate this effect; it is imperative for corporations to implement security measures to handle such risks.

The thesis discusses how to build a secure corporate network, what means are there to enhance it, how the installation of MobiControl is conducted in a Windows server environment and how to establish a LDAP connection to the Active Directory server. The implementation also covers how the enrollment of Android and Windows phones is carried out via an HTTPS connection to the production server outside the corporate network.

The result of the thesis, the implementation of SOTI MobiControl is at the time of writing already used in several devices inside the company. Currently Medbit is also looking into other MDM solutions mainly from the Citrix product family, as large numbers of clients use Citrix software.

KEYWORDS:

SOTI, MDM, AD, DA, Android, Windows, MobiControl, LDAP, Port Forward, IP

SISÄLTÖ

KUVAT

TAULUKOT

KÄYTETYT LYHENTEET

.NET	Microsoftin kehittämä sovelluskehys
AD	Active Directory, Windows-toimialueen tietokanta, joka sisältää käyttäjätiedot.
DA	Device Agent, Käyttäjäagentti, joka asennetaan älypuhelimiin, jotta MobiControl pystyy hallitsemaan sitä
HTTP	Hypertext Transfer Protocol, selaimien ja WWW-palvelimien käyttämä tiedonsiirtomenetelmä
HTTPS	Hypertext Transfer Protocol Secure, HTTP-yhteys, joka on suojattu SSL-menetelmällä
IP	Internet Protocol TCP/IP-mallin protokolla, joka huoleh tii, että paketit pääsevät perille Internetissä
LDAP	Lightweight Directory Access Protocol, verkkoprotokolla, jota käytetään hakemistopalveluissa.
MDM	Mobile Device Management, älypuhelimien hallintaan käytettävä ratkaisu
SMTP	Simple Mail Transfer Protocol, viestin välittämiseen sähköpostipalvelimien kesken käytetty protokolla
SSL	Secure Socket Layer, salausprotokolla, jolla salataan tietoliikenne
TCP	Transmission Control Protocol, protokolla, jonka avulla luodaan yhteyksiä tietokoneiden välillä Internetissä
UDP	User Datagram Protocol, protokolla joka mahdollistaa tiedostojen siirron, mutta ei vaadi yhteyttä.

1 JOHDANTO

MDM eli Mobile Device Management on puhelimien, älypuhelimien, tablettien ja kannettavien tietokoneiden hallintaan tarkoitettu työkalu. MDM:n avulla turvataan, seurataan, hallinnoidaan ja tehostetaan päätelaitteiden toimintaa ja turvallisuutta. MDM:n avulla pidetään yrityksen tiedot lukittuina ja turvassa päätelaitteissa sekä varmistetaan, että tieto ei pääty väärin käsiin. (TechTarget 2013.)

Mobiililaitteiden ja etenkin älypuhelimien yleistyessä työpaikoilla yhä useampi henkilö käyttää päätelaitteita työajan ulkopuolella. Monet yrityksissä työskentelevät käyttävätkin yritykseltä saatuja puhelimiaan henkilökohtaisissa asioissa ja asettavat näin huomaamattaan yrityksen tiedot, sähköpostit ja tiedostot varastamisen tai monen muun tietoturvauhan kohteeksi. Tämän ongelman ratkaisemiseksi on rakennettu MDM-ratkaisuja, joiden avulla hallinnoidaan älypuhelimia, mobiililaitteita sekä kannettavia tietokoneita. MDM:a käyttämällä pidetään huoli, että oikeat sovellukset on asennettu päätelaitteille, mahdollistetaan turvallinen pääsy yrityksen tiedostoihin sekä tarpeen vaatiessa otetaan laite hallintaan etäyhteydellä (Ellis ym. 2012, 1–2.)

Elmira Bagheri Majdi opinnäytetyössään ”Evolution of Mobile Device Management Tools and Analysing Integration Models for Mobility Enterprise” Käy läpi MDM-tuotteen markkinoita, käyttötarkoitusta ja merkitystä yrityksen tietoturvan kannalta. Bagheri mainitsi mm. MDM-tuotteiden tärkeyden älypuhelimien hallinnassa. Sillä älypuhelimien käyttö työpaikalla yleistyy jatkuvasti näin luoden paikoittain suuria tietoturvallisuusriskejä yrityksille. Huomasin omassa työssäni täysin samat asiat sekä sen miten ajankohtainen MDM-tuotteiden käyttöönotto on. (Bagheri, 2013, 18)

Opinnäytetyön tavoitteena on toteuttaa toimiva MDM-ratkaisu Medbit Oy:n käyttöön ja saada onnistuneesti rekisteröityä Android- sekä Windows-pohjaisia älypuhelimia hallintajärjestelmään. MDM-ratkaisua tullaan käyttämään sovellusten etäasennukseen ja päivittämiseen, laitteiden jäljittämiseen sekä varkauksien varalta laitteen lukitsemiseen ja tyhjennykseen. Aiemmin sovelluksen asenta-

mista varten laite on pitänyt tuoda takaisin Medbit Oy:lle ja manuaalisesti hoitaa sovelluksien asentaminen ja päivittäminen.

Medbit Oy on valinnut käyttöönotettavaksi SOTI:n tarjoaman MobiControl-ohjelmiston sen WWW-pohjaisen hallintajärjestelmän ja Windows-ympäristönsä vuoksi. MDM:n asennus toteutetaan asentamalla MobiControl-järjestelmä Windows 2012R2 -palvelimelle, joka sijaitsee konesalissa ja jossa on .NET 4.5 -sovelluskehys ja MS SQL 2012 -tietokanta.

Älypuhelimien hallinta tapahtuu WWW-pohjaisen hallintapaneelin kautta. Tästä syystä opinnäytetyön luvussa 2 käsitellään, mitä on verkkosuojaaminen ja mitä menetelmiä sekä suojauskeinoja käytetään turvallisen yritysverkon rakentamiseen. Läpikäytyjen menetelmien avulla luodaan turvallinen verkkoympäristö älypuhelimien hallintaa varten ja turvataan, että verkkoon ei pääse tunkeutumaan helposti esim. hyväksikäyttämällä avoinna olevia portteja. Luvussa 3 käsitellään MobiControllin tärkeitä ominaisuuksia ja älypuhelimien hallintaan liittyviä ohjelmistoja. Luvussa 4 käydään läpi MobiControllin asennus Windows-palvelimelle ja lisätään päätelaitteet ohjelmistoon. Windows-pohjaisten laitteiden lisäämistä varten käydään lisäksi läpi, miten luodaan LPAD-yhteys verkon Active Directory -palvelimeen.

Opinnäytetyö toteutetaan vakituisessa työsuhteessa Medbit Oy:ssä. Medbit Oy on vuonna 2008 perustettu julkisomisteinen osakeyhtiö, joka tuottaa keskitetysti Satakunnan, Vaasan ja Varsinais-Suomen sairaanhoitopiirien alueen terveydenhuollon ja sosiaalihuollon organisaatioiden tarvitsemat ICT-palvelut. (Medbit Oy 2015)

2 VERKKOSUOJAUS

Verkkosuojaaminen viittaa mihin tahansa toimintaan tai aktiviteettiin, joka suojaa yrityksen verkkoa. Verkkoa suojataan useimmiten mm. viruksilta, vakoilu- ja mainosohjelmilta, hakkerihyökkäyksiltä, palvelunestohyökkäyksiltä, identiteettivarkaudelta ja datan varastamiselta. Näiden hyökkäysten estämiseksi tulee olla rakennettu monipuolinen tietoturvataso. Yrityksen tietoturvaa ylläpidetään laitteistojen ja tietokoneohjelmistojen avulla, josta tietokoneohjelmistoja on päivitettävä tasaisin väliajoin. (Pinzon 2015.)

Verkko voi koostua monesta eri tietokoneesta tai muusta laitteesta, jotka ovat kytkettynä toisiinsa ja voivat jakaa tietoa sekä keskustella toistensa kanssa. Näitä verkkoja rakennetaan käyttämällä monia eri keinoja: kaapeleiden kautta kuten Ethernet-kaapelin, puhelinverkkojen, satelliittien, radioaaltojen sekä infrapunasäteiden kautta. Yrityksen verkko koostuu pääasiallisesti kytkimistä, reitittimistä, langattomista verkoista, palomuureista ja palvelimista sekä tietokannoista, joissa yrityksen tiedot sijaitsevat. (Networking Basics 2015.)

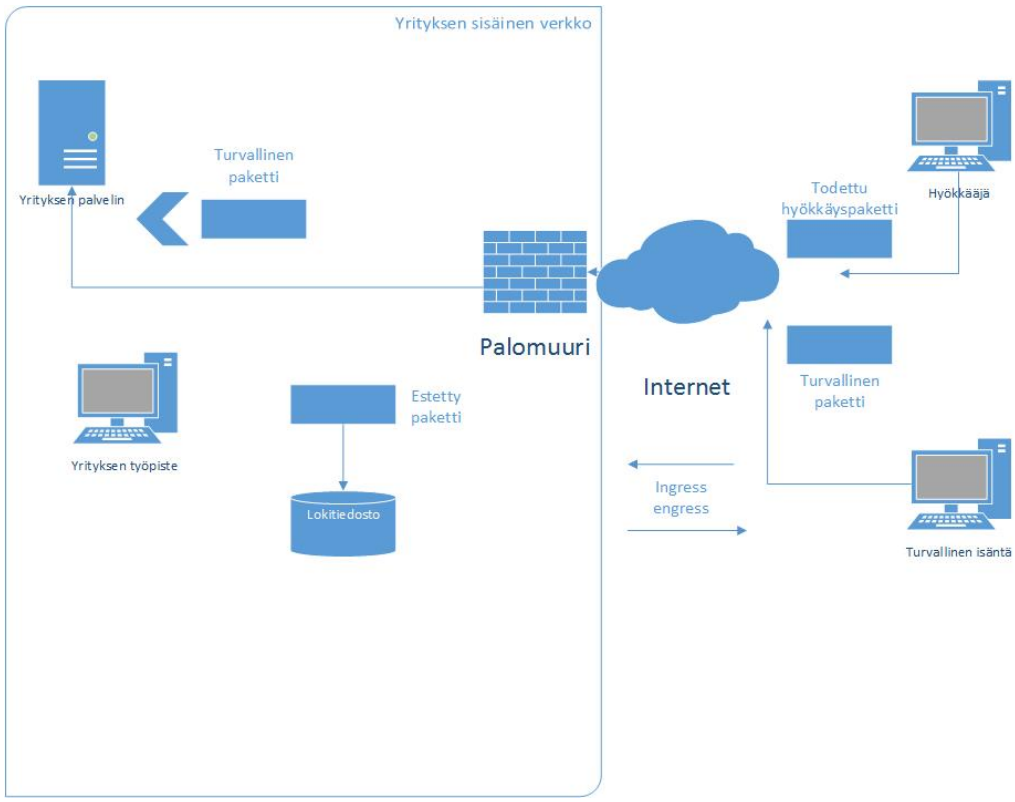
2.1 Palomuuri

Palomuuri on ohjelmisto, joka suodattaa tietoliikennettä kahden eri verkon välillä. Palomuuri tarkastelee tulevaa ja poismenevää liikennettä ennalta määrättyjen turvallisuussääntöjen perusteella. Kaikki tulevat paketit menevät palomuurin lävitse. Jos palomuuri havaitsee, että paketti on haitallinen, hylkää palomuuri kyseisen paketin pääsyn verkkoon. Jos paketti on puolestaan turvallinen, päästää palomuuri sen verkkoon (Kuva 1). (Boyle & Panko 2012, 314.)

Palomuuri perustaa seinämän sisäisen turvallisen verkon ja toisen ulkopuolisen verkon kanssa, kuten Internetin, joka on oletukseltaan ei-luotettava tai ei-turvallinen. Paketit, jotka on merkitty uhkaaviksi, tallennetaan lokitiedostoon. Tätä menetelmää kutsutaan lokittamiseksi. Lokitiedostosta järjestelmänvalvojan pitää päivittäin katsoa, mitä paketteja on mennyt läpi ja mitä ei, jotta ymmärtää,

millaisia hyökkäyksiä kohdistuu yrityksen palomuuriin. (Boyle & Panko 2012, 314.)

Yrityksellä voi olla monia palomuureja, jotka suojaavat niin sisäiseltä kuin ulkoiselta liikenteeltä. Border-palomuurit suojaavat verkkoa ulkoiselta maailmalta, kun taas sisäistä liikennettä suodattavat sisäiset palomuurit. (Boyle & Panko 2012, 314.)



Kuva 1. Palomuuri suodattaa paketteja (Boyle & Panko 2012, 314).

2.1.1 Ingress-suodatus

Ingressi-suodatus tarkoittaa sitä, kun palomuuri tarkastelee liikennettä, joka koittaa tulla ulkoisesta verkosta, tyypillisesti Internetistä tai muusta ei-turvallisesta paikasta. Ingress-suodatuksen tarkoitus on estää pakettien pääsy sisäverkkoon ja säästää näin verkkoa mahdolliselta saastumiselta. (Boyle & Panko 2012, 314.)

2.1.2 Engress-suodatus

Egress-suodatuksessa palomuuri suodattaa paketteja, jotka poistuvat verkosta. Tämä estää ns. Probe-pakettien lähtöä verkosta. Paketit tutkivat verkon rakennetta ja ottavat selville, mitkä portit ovat suojattuja ja mitkä ei. Näin palomuuri estää virusten tai haitallisten matojen leviämiseen muihin verkkoihin ja Internetiin. (Boyle & Panko 2012, 314–315.)

2.2 Portit

Portti on osoite, jonka kautta tietynlainen tietoliikenne kulkee. Portteja on määritelty porttinumerosta 1 aina 65535:een asti TCP-protokollaa käyttämällä OSI-mallin neljännessä, eli kuljetuskerroksessa. Kuljetuskerroksessa (Transport Layer) sallitaan tietojenvälitys lähde- ja kohdekoneiden välillä. Tässä kerroksessa tieto kulkee Internetissä paketteina. Näistä on tehty tarkkoja sääntöjä, joita kutsutaan protokolliksi. Näiden protokollien ja pakettien vuoksi muut tietokoneet voivat tunnistaa paketit dataksi ja purkaa koodauksen, minkä jälkeen data pääsee perille. Eri sovellukset käyttävät erilaisia portteja tai kanavia siirtääkseen tämän datan. (Dye ym. 2008 103–104.)

Yleisesti yhtä porttia käytetään datan lähettämiseen ja toista sen vastaanottamiseen. Jokaisella paketilla on ilmoitettu header-osiossaan, minkä portin kautta sen tulee kulkea. Jos paketit kuitenkin törmäävät toisiinsa, ne joko hylätään tai lähetetään uudelleen, jos kuittausta ei tule. Näin ollen ei synny datahukkaa ja paketit pääsevät perille, kuten on alun perin pitänytkin. Taulukossa 1 on esitetty tunnetuimmat portit, joita käytetään. (Dye ym. 2008 108.)

Taulukko 1. Tunnetuimmat portit (Boyle & Panko 2012, 332).

Portti	Protokolla	Applikaatio
20	TCP	FTP Data Traffic
21	TCP	FTP Supervisory Connection
22	TCP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	SMTP
53	TCP	DNS
69	UDP	TFTP
80	TCP	HTTP
110	TCP	POP
135–139	TCP	NETBIOS
143	TCP	IMAP
161	UDP	SNMP
443	TCP	HTTP over SSL/TSL
3389	TCP	RDP

Juuri porttien avulla palomuurin läpi menevää liikennettä hallinnoidaan ja seurataan. Portteja voi hallinnoida palomuurin kautta, ja niitä voi sulkea ja avata tarpeen mukaan. Portit toimivat ”kuuntelemalla” ja odottamalla, että dataa saapuu avatusta portista. Avoimet portit ovat mainioita kohteita, joiden kautta hyökätään verkkoon. Tämän vuoksi on tärkeää, että järjestelmänvalvoja tietää tarkkaan, mitä portteja on avattu, ja sulkee tarpeettomat portit. (Pinzon 2015.)

Internetin sisältö erotetaan toisistaan sovellusten ja niille määrättyjen porttien avulla. Yleisimmät laajasti käytetyt protokollat ovat

- WWW-yhteys käyttämällä HTTP-protokollaa
- sähköposti käyttäen SMTP-protokollaa
- FTP-Tiedonsiirtomenetelmä
- DNS-palvelimien käyttö.

- Terminaaliyhteydet kuten VNC, Telnet ja Secure Shell

Porttien avulla pystytään siis erottamaan toisistaan esim. WWW-sivut ja sähköposti sovelluskerroksessa, sillä kaikilla on oma portti, jonka kautta kyseisen palvelun liikenne liikkuu Internetissä. (Pinzon 2015.)

Porttien avaamisien avulla ohjataan liikennettä ulkopuolisesta maailmasta osoitettuun palvelimeen paikallisessa TCP/IP-verkossa. Internet-palvelut tunnistetaan standardisoitujen porttien mukaan, esimerkiksi WWW-liikenne käyttää porttia 80. Portteja avataan sekä suljetaan palomuurissa, mikä määrittää palomuurin läpi pääsevän liikenteen sekä saapuvan liikenteen ohjaamisen (Definition of: Port Forwarding 2015.)

2.3 SSL

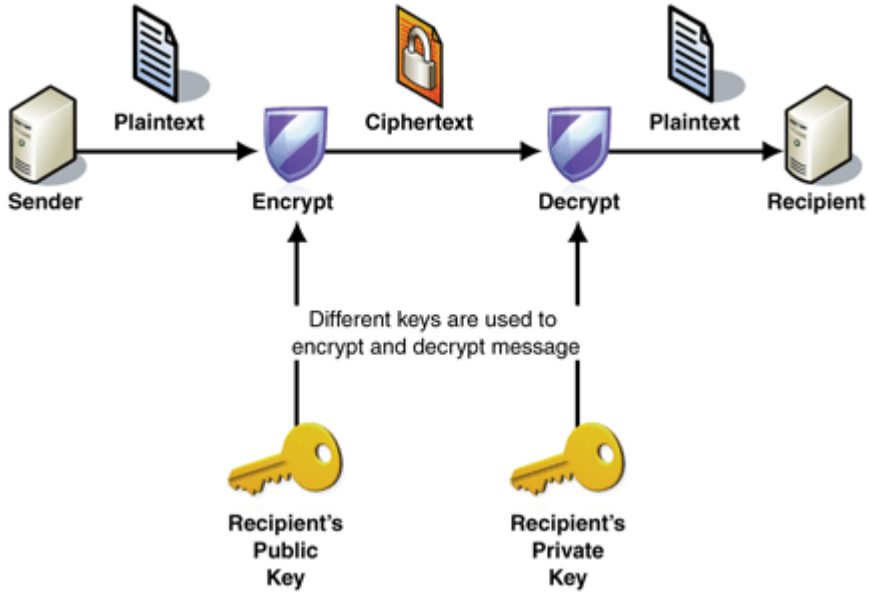
Secure Sockets Layer (SSL) on kryptografinen salausmenetelmä, joka ilmestyi jo 1990-luvulla Netscapen kehittämänä. SSL luo salatun yhteyden käyttäjän selaimen ja WWW-palvelimen välillä suojaten samalla kaiken liikenneyhteyden, joka tapahtuu palvelimen ja käyttäjän välillä. SSL-yhteyden avulla arkaluonteista tietoa kuten luottokorttien numerot, henkilötunnukset ja käyttäjätunnukset sekä salasanat voidaan välittää turvallisesti. (Digicert 2015.)

Ensin SSL-salauksessa kysytään varmenne, joka pitää joko ladata tai hyväksyä. Seuraavaksi SSL-salauksen avulla suojataan ja luodaan turvallinen, salattu yhteys verkkoasiakkaan sekä palvelimen välillä käyttäen salausalgoritmia sekä julkista salausavainta. WWW-pohjaisissa vuorovaikutuksissa SSL-salausmenetelmä salaa ja suojaa datan siirtyvyyden Secure Hypertext Transfer-protokollaa käyttäen. (Digicert 2015.)

Transport Layer Security (TLS)-protokolla on otettu käyttöön, sillä SSL-protokolla on todettu epäturvalliseksi. SSL v3.0 on todettu turvattomaksi sillä tietoturvauhat kuten POODLE ja BEAST ovat osoittaneet, että kyseinen salausmenetelmä on täysin turvaton. Tietoturvauhkien paikkaamiseksi on kehotettu, että päivitettäisiin TLS V1.1 tai TLS V1.2-salausmenetelmiin. (Kangas 2008.)

2.3.1 Epäsymmetrinen salaus

Epäsymmetrisessä salauksessa osapuolet käyttävät PKI-avainparia salatun yhteyden luomiseksi palvelimen ja käyttäjän välillä. Yksi avaimista on julkinen (public key) ja vastaavasti toinen on yksityinen (private key). Julkisen avaimen avulla salataan teksti mikä halutaan lähettää verkkoliikenteen yli salakirjoitukseksi. Tämä salaviesti voidaan avata vain kyseisellä vastakkaisella yksityisellä avaimella sekä päinvastoin. Kuvassa 2 demonstroidaan miten epäsymmetrinen salaus toimii. (Horman 2005.)

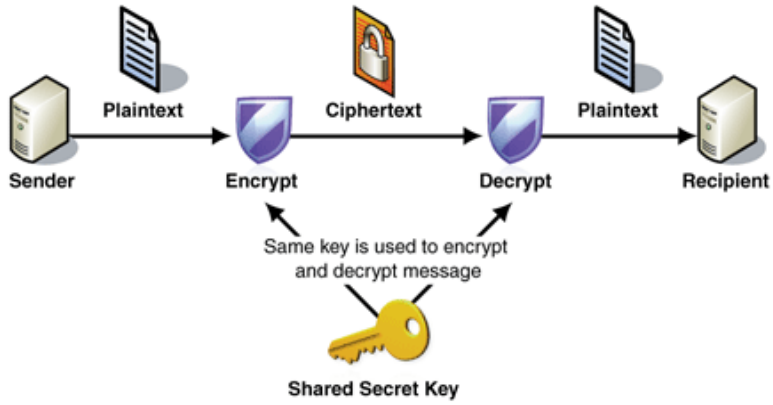


Kuva 2. Epäsymmetrinen salausmenetelmä (Microsoft 2005).

2.3.2 Symmetrinen salausmenetelmä

Symmetrisessä salauksessa käytetään vain yhtä avainta tiedon salaamiseen ja purkamiseen. Tämä menetelmä on yksinkertaisempi ja nopeampi kuin epäsymmetrinen salaus, sillä tietojen salaus ja purkaus tehdään samalla julkisella avaimella. Yleisesti käytettyjä symmetrisiä salaus algoritmeja ovat DES, sen seuraaja DES3 ja uusimpana AES. Kuvassa 3, nähdään miten symmetrinen salaus toimii (Horman 2005).

Samaa julkista avainta käytetään purkaukseen ja salaukseen. Jos avain päätyy kolmannen osapuolen tietoon, voi osapuoli luoda tekaistuja salattuja viestejä ja purkaa siepattuja viestejä. Tämän vuoksi on tärkeää, että julkinen avain jaetaan osapuolten kesken turvallisesti. (Horman 2005.)



Kuva 3. Symmetrinen salausmenetelmä (Microsoft 2005).

2.4 Virtual Private Network

VPN eli Virtual Private Network on keino, jonka avulla muodostetaan salattu yhteys kahden eri suljetun verkon välillä Internetin yli. VPN luodaan käyttämällä kryptografista järjestelmää liikenteen turvaamiseen ja datan siirtoa tietoliikenneverkon yli, mikä on vailla tietoturvallista allekirjoitusta, kuten Internetin taikka langattomien verkkojen yli. VPN-yhteyksien luomisessa käytetään SSL/TLS-salausmenetelmää. Se sallii käyttäjän lähettää ja vastaanottaa dataa julkisten taikka jaettujen verkkojen yli ihan kuin oma tietokone olisi suoraan yhteydessä yrityksen yksityiseen verkkoon. VPN siis suojaa yhteyden, joka on muodostettu julkisen Internetin yli. Suojauksen avulla käyttäjä hyötyy yksityisen verkon toiminnasta, sen turvallisuudesta ja mahdollisista tietojärjestelmistä, joihin on pääsy vain yrityksen sisäverkosta. (Boyle & Panko 2012, 172–174.)

VPN-yhteyttä voidaan käyttää host-to-host-periaatteella, jossa luodaan vain yksittäinen VPN-yhteys oman tietokoneen ja palvelimen välillä ei-luotettavan verkon yli. Remote access-periaatteessa luodaan VPN-yhteyden avulla salattu yhteys luottamattoman verkon yli suoraan yrityksen sisäiseen verkkoon. Site-to-

site VPN-yhteydessä otetaan VPN-yhteys kahden yksityisen verkon väliltä. Tässä yhteydessä kaikki liikenne on salattua verkkojen välillä. (Boyle & Panko 2012, 172–174.)

2.5 HTTPS-protokolla

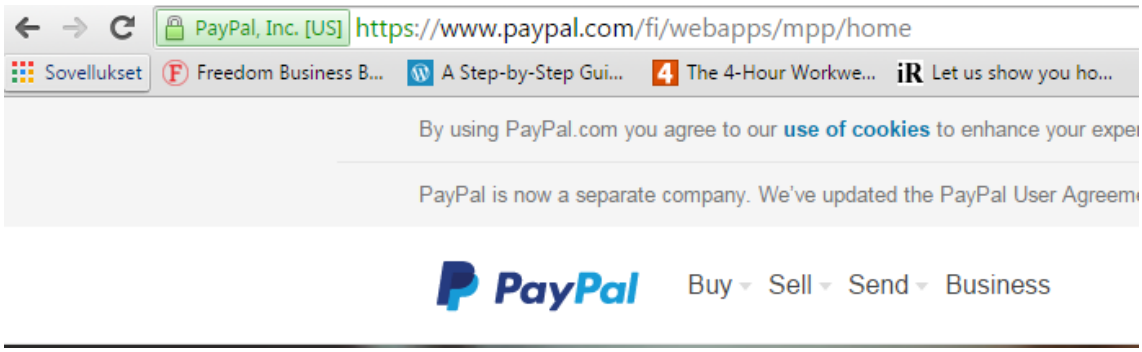
HTTP-protokollan käyttöönoton lisääntymisen myötä on tarvittu salausmenetelmä, joka onnistuneesti pystyy salaamaan datan siirron Internetissä. SSL/TLS-salausmenetelmät kehitettiin tuomaan lisäturvallisuutta ja suojaa, jotta dataa ei päätyisi väärin käsiin. HTTPS on HTTP-protokollaan perustuva tiedonvälitysmenetelmä, mutta se on suojattu SSL/TLS-salausmenetelmällä. Ennen HTTP-kutsun lähettämistä HTTPS-yhteydessä tiedot salataan SSL/TLS-salausmenetelmällä. (RTFM 2000.)

HTTPS-käyttää symmetristä salausmenetelmää ja näin on vaarana, että ei voida takuuvarmasti tunnistaa, onko vastapuoli se, joka hän väittää olevansa. Tämän vuoksi tarvitaan digitaalinen allekirjoitus sertifikaattiin luotetulta kolmannelta osapuolelta, joka varmistaa, että kyseinen sertifikaatti kuuluu verkkotunnuksen omistajalle. Verkkotunnuksella tarkoitetaan Internet-osoitetta, jota käytetään kotisivujen ja sähköpostilaatikoiden osoitteina. Sertifikaatit perimmiltään liittävät yhteen verkkotunnukset niihin kuuluviin julkisiin avaimiin, joita ne käyttävät. Edellyttäen, että keskivertainen selain ”luottaa” tähän sertifikaattiin, siinä on oltava Certificate Authorityn (CA) allekirjoitus. CA-varmentajat ovat yhtiöitä, jotka suorittavat manuaalisen tarkistuksen, että hakeva osapuoli on

- oikea ihminen tai yritys, joka on olemassa julkisissa tiedostoissa
- omistavat verkkotunnuksen, johon he ovat hakemassa allekirjoitettua sertifikaattia.

Edellä mainittujen asioiden varmistuttua CA myöntää ja allekirjoittaa verkkotunnuksen sertifikaatin ja antaa hyväksyntänsä, että julkinen avain kuuluu kyseiselle verkkotunnukselle. Jos verkkotunnus on saanut hyväksytyn allekirjoituksen

CA:lta, näkyy selaimessa vihreä palkki, lukko ja HTTPS-alkuinen osoite kuten on demonstroitu kuvassa 4. (Brody 2013.)



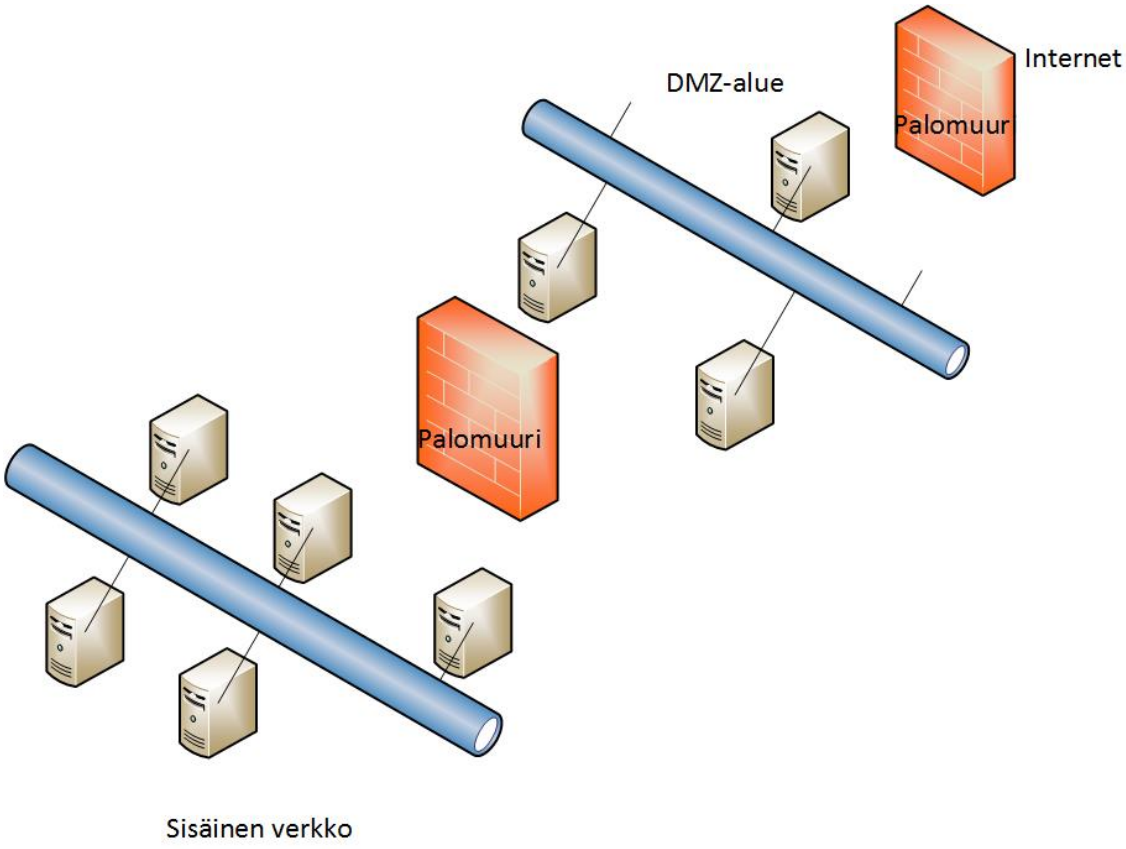
Kuva 4. HTTPS-suojattu verkkosivu

2.6 DMZ-verkko

DMZ eli demilitarisoitu vyöhyke on palomuurin suojaama alue, johon voidaan ottaa yhteys ulkoisesta maailmasta. DMZ:n avulla erotetaan yrityksen sisäinen verkko muusta vaarallisesta ja turvattomasta verkosta kuten Internetistä. DMZ siis yhdistää yrityksen omat järjestelmät turvattomaan verkkoon, toimimalla yhteysverkostona näiden välillä kuvan 5 osoittamalla tavalla. DMZ:n tarkoitus on lisätä ylimääräistä tietoturvatasoa yrityksen sisäiseen verkkoon. (Shinder 2005.)

DMZ:n sisälle laitetaan pääsääntöisesti palvelimet, jotka tarvitsevat yhteyden ulkomaailmaan. Jos yrityksen sisäisessä verkossa on näitä palvelimia, voidaan kyseisiä julkisia palvelimia kohti suunnata hyökkäyksiä tai kaappauksia. Jos palvelin saadaan haltuun DMZ-alueen sisällä, uhka jää vain kyseiselle alueelle ja se suljetaan pois kokonaan yrityksen sisäisestä verkosta. Kaksi tärkeintä asiaa, jotka tulee tietää, kun pystyttää DMZ-aluetta, on (Shinder 2005.)

- DMZ-verkolla on eri verkkotunniste kuin yrityksen sisäisellä verkolla
- DMZ-verkon erottaa sisäisestä verkosta ja julkisesta verkosta palomuurin avulla.



Kuva 5. DMZ sijoittuu "epäluotettavan" Internetin ja yrityksen sisäisen verkon välissä. (Shinder 2005.)

3 SOTI MOBICONTROL -TUOTERATKAISU

SOTI MobiControl on SOTI:n tarjoama Enterprise Mobility Management -tuoteratkaisu (EMM), jonka avulla hallitaan mobiililaitteita, älypuhelimia ja tietokoneita. MobiControl-ratkaisu tarjoaa mahdollisuuden hallita turvallisesti mobiililaitteisiin kytkettyjä oheislaitteita, sovelluksia, sisältöä ja sähköposteja. MobiControllin tarjoaman turvallisuuden ja hallintaominaisuuksien takia yrityksellä on selvä käsitys, miten ja mihin laitteita käytetään. (SOTI 2015a.)

MobiControl tukee seuraavia alustoja: Windows Mobile, Windows, Android, Android for Work ja Apple iOS (SOTI 2015a).

MobiControlliin kuuluu viisi eri komponenttia, joista koko mobiilihallinta koostuu (Kuva 6). Komponentteja ovat (SOTI 2015a.)

- Web Console, jonka kautta hoidetaan suurin osa toiminnoista liittyen mobiililaitteen hallintaan
- Deployment Server, joka kommunikoi mobiililaitteiden kanssa ja suorittaa asetetut säännöt
- Device Agent –ohjelmisto, joka on asennettuna mobiililaitteisiin ja kommunikoi Deployment -palvelimen kanssa ja hoitaa sovelluspakettien asentamisen sekä poistamisen
- Package Studio, jossa luodaan erilaisia sovelluspaketteja mobiililaitteelle.
- tietokanta, jossa säilytetään tieto laitteiden kunnosta ja rakenteesta sekä kaikista sovelluspaketeista, joita on tehty.

Kuva 6. SOTI MobiControl rakenne (SOTI 2015c, 2).

3.1 Tärkeimmät ominaisuudet

MobiControllissa tärkeimmät ominaisuudet keskittyvät laitteen hallintaan, suojaukseen ja etäpaikannukseen. Kaikkien tärkeimpien ominaisuuksien myötä rakentuu kokonaisuus, jonka avulla mobiililaitteiden hallinta on turvallista, helppoa ja tehokasta. Näiden toimintojen vuoksi MobiControllia käytetään ympäri maailmaa ja jo yli 14 000 aktiivista laitetta hallitaan sovelluksen kautta. (SOTI 2015b.)

3.1.1 Paikannus

Paikannustoimintojen ohella pystytään myös jäljittämään, seuraamaan, asettamaan tietyt rajat, joiden ulkopuolelle mobiililaite ei saa mennä ja tarkkaan ottaen katsoa, mitä reittejä pitkin laite on kulkenut. Paikannuksen myötä yrityksellä on täysi tieto, missä laite liikkuu ja milloin. Varkauden tapahtuessa tiedetään tarkkaan, missä laite on. Paikannus toimii käyttämällä puhelimen GPS-vastaanotinta satelliitin avulla. (SOTI 2015b.)

3.1.2 Virustorjunta

MobiControllin avulla eristetään uhat, virukset sekä haittaohjelmat. Näin saadaan turvattua mobiililaitteen tärkeimmät tiedostot ja estetään niiden saastuminen. Virustorjuntaominaisuuksien kannalta saadaan mobiililaitteisiin asennettua työpisteen tasoinen tietoturvasuojaus. Virustorjunta tutkii jokaisen asennetun sovelluksen ja komentosarjan, joka asennetaan älypuhelimiin. Haitallisen ohjelman löydyttyä se eristetään omaan tilaansa, jonka jälkeen se poistetaan. (SOTI 2015b.)

3.1.3 Tietoturva ja lähituki

Tietoturvasta huolehditaan asettamalla rajoituksia: mitä sovelluksia on lupa ladata, millä sivuilla voidaan vierailla ja seuraamalla tarkkaan, miten data liikkuu älypuhelimessa. Datan seuranta ja etähallinta perustuvat DA:n toimintaan, sillä sovelluksella on järjestelmänvalvojan oikeudet kaikkiin toimintoihin älypuhelimessa. (SOTI 2015b.)

MobiControllin avulla voidaan ottaa etäyhteys mobiililaitteeseen ja suorittaa tarpeen mukaan päivitykset sekä sovelluksien asennukset käsin. Etähallinta onnistuu vain Windows- ja Android For Work -pohjaisissa laitteissa.

3.1.4 Sovellusten hallinta

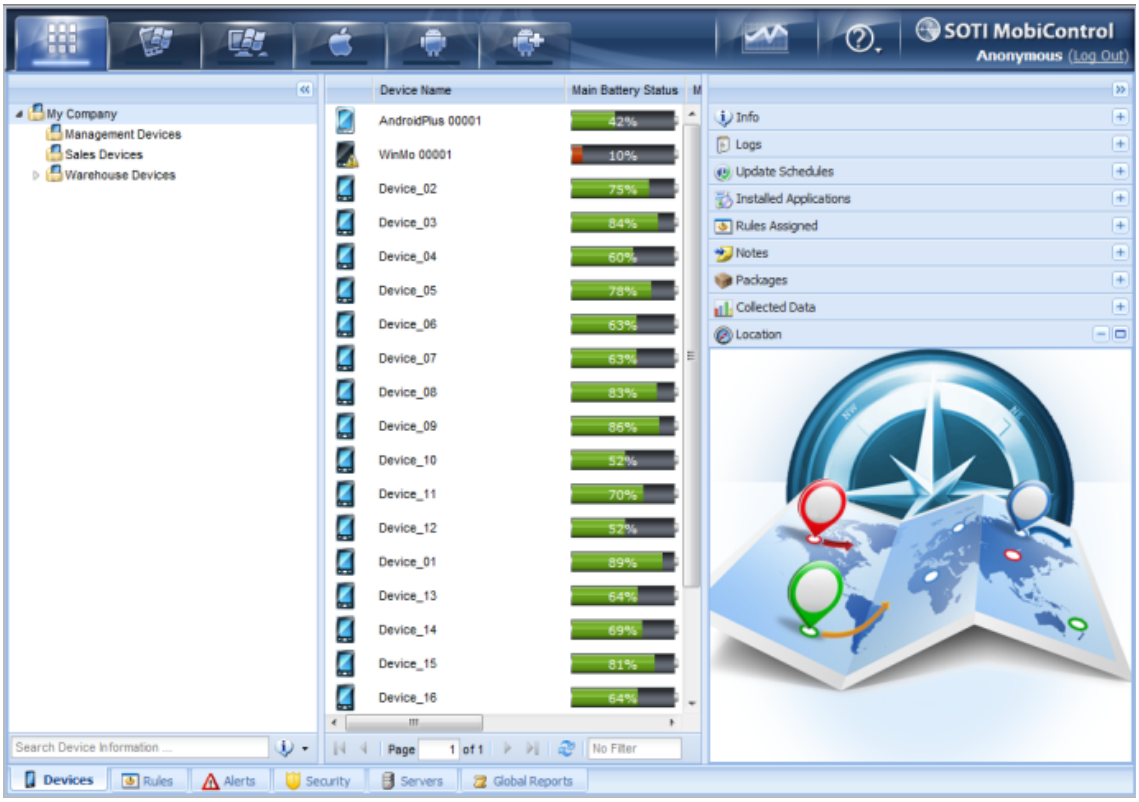
Sovellusten hallinta on tärkeässä osassa MobiControllin toimintaa. Sovellusten hallinta perustuu sovelluspolkujen perusteella asetettaviin estoihin. Ensin Web Consolesta määritetään ohjelma ja sen sovelluspolku, jota halutaan hallita. Tämän jälkeen sovellusta voidaan seurata tai rajoittaa sen toiminta kokonaan. (SOTI 2015c .)

Sovelluksia hallitaan oman käyttöliittymän kautta ja näin voidaan tarkkaan määrittää, mitä sovelluksia laitteissa on. Mobiililaitteisiin voidaan näiden avulla asentaa mitä tahansa sovelluksia, olkoon kyseessä yrityksen omat sovellukset tai Google Play-kaupasta peräisin olevat sovellukset. Kaikki tieto, joka liikkuu älypuhelimien ja tuotantopalvelimien välillä on SSL-suojattua. (SOTI 2015b.)

3.2 Web Console

MobiControllin WWW-hallintapaneelin eli Web Consolen avulla hallitaan kaikkia yrityksen mobiililaitteita ja asetetaan säännöt sekä rajoitukset, jotka tulevat koskemaan älypuhelimia. Hallintapaneelia voi käyttää millä tahansa laitteella, sillä käyttämiseen tarvitaan vain Internet-selain. Hallintapaneelin kautta voidaan tehdä seuraavia asioita (SOTI 2015b.)

- asettamaan sääntöjä, joiden mukaan rekisteröityminen tapahtuu
- sääntölinjauksia, esteitä ja rajoituksia
- paikantamaan ja ottamaan etähallintaan mobiililaite
- komentosarjojen ja erilaisten viestien lähettäminen
- raporttien teko
- tarkastelemaan tuotantopalvelimen asetuksia
- katsomaan kootusti kaikkia laitteita, joita hallinnoidaan. (Kuva 7)

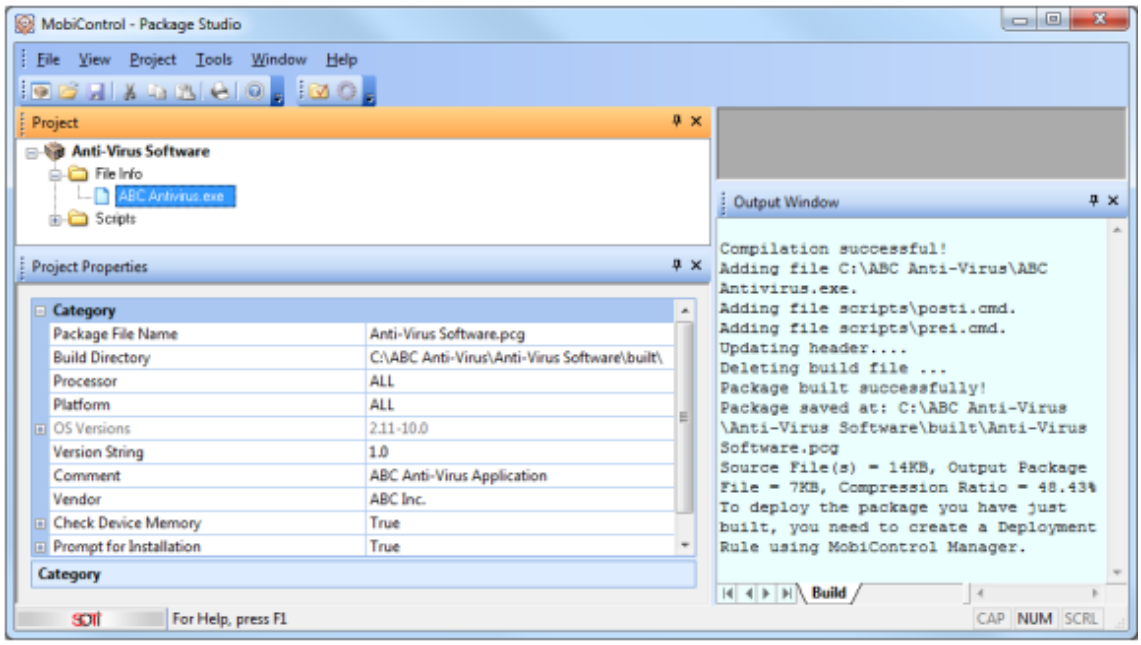


Kuva 7. Web-Consolen Devices -näkymä (SOTI 2015d).

3.3 Package Studio

Package Studiota käytetään luomaan sovellus- tai datapaketteja, jotka asennetaan mobiililaitteille (Kuva 8). Paketti on yksinkertaisesti sarja tiedostoja, jotka ovat tiivistetty yhteen tiedostoon. Tiivistetyt paketit antavat mahdollisuuden jakaa paketteja nopeammin mobiililaitteille ja mahdollistavat datan jakamisen hitailla verkkoyhteyksillä. Onnistuneesti rakennetut paketit käyttävät päätettä .pcg. (SOTI 2015c, 414.)

Tavallisten pakettien lisäksi Package Studion avulla paketteihin voi liittää erilaisia komentosarjoja, joita halutaan toteuttaa päätelaitteilla. Komentosarjat suoritetaan automaattisesti pakettien asennuksien tai poistojen yhteydessä. Package Studion avulla on myös mahdollista luoda paketteja, jotka sisältävät pelkästään komentosarjoja toteuttamaan tiettyjä toimintoja tai komentoja. Studion avulla myös saadaan automaattisesti cab, .reg tai .exe-päätteisiä tiedostoja käynnistymään asennuksen tai poiston yhteydessä. (SOTI 2015c, 414.)



Kuva 8. Onnistunut paketin luominen Package Studion kanssa (SOTI 2015c, 414).

3.4 Soti Administrator Utility

Administrator Utility on ohjelmisto, joka antaa järjestelmänvalvojalle keskitetyn näkymän, minkä avulla seurataan tuotanto-palvelimen toimintoja, missä MobiControl sijaitsee. Tämän ohjelmiston kautta järjestelmänvalvoja voi

- tarkistaa, ovatko kaikki ohjelmiston komponentit toiminnassa
- tarkistaa komponenttien tilannetta ja testata palvelimen ominaisuuksia
- tarkistaa ja testata tuotanto-palvelimen toimintoja
- säätää WWW-hallintapaneelin yhteydenottoportteja
- konfiguroida palvelimen sertifikaatteja
- konfiguroida tietokantayhteyksiä tuotantopalvelimella

Administrator Utilityn kanssa ohjataan koko MobiControllin palvelimiin liittyviä toimintoja, eli varmistetaan sertifikaattien laillisuus, asetetaan oikeat IP-osoitteet tuotantopalvelimelle, päätelaitteiden rekisteröintiä ja hallinnoidaan porttien avaamisia. Utilityn avulla asetetaan, mitä portteja palvelin kuuntelee, kun halutaan päästä WWW-hallintapaneeliin ja kun halutaan yhteys tuotanto-

palvelimeen. WWW-hallintapaneelin pääsee käsiksi HTTP- tai HTTPS-protokollien kautta, mutta tuotanto-palvelin ottaa vastaan kutsuja vain portilta 443, eli HTTPS-suojattuja kutsuja. (SOTI 2013.)

3.5 Device Agent

MobiControllin Device Agent (DA) on Mobicontrollin ohjelmisto, joka asennetaan älypuhelimiin. DA kommunikoi MobiControllin tuotantopalvelimien kanssa ja on vastuussa Package Studion luotujen pakettien asentamisesta sekä poistamisesta älypuhelimissa. DA toimittaa tuotantopalvelimelle reaaliaikaista dataa älypuhelimen toiminnasta ja sijainnista. Näin DA yhdistää ja rekisteröi kaikki yrityksen älypuhelimet MobiControllin keskitettyyn hallintajärjestelmään, Web-Consoleen. DA asennetaan ensin rekisteröimällä laite tuotantopalvelimelle, minkä jälkeen asennusohjeiden mukaisesti ladataan sovellus Googlen Play-kaupasta. (SOTI 2015c, 278)

4 SOTI MOBICONTROL KÄYTTÖÖNOTTO

Käyttöönoton yhteydessä Medbit Oy on määrittänyt ominaisuuksia, joiden pitää onnistua MobiControllin avulla. Näitä vaatimuksia ovat WLAN-yhteyksien vieminen älypuhelimeen, sovellusten asennus sekä päivitys, laitteen paikantaminen ja lukitseminen sekä erilaisten sääntöjen luominen, miten saadaan rajoitettua älypuhelimien käyttöä esim. estämällä tiettyjen sovelluksien asentamisen älypuhelimelle. MobiControllin avulla hallitaan Medbitissä vain Android- ja Windows-käyttöjärjestelmiin pohjautuvia älypuhelimia. Tämän vuoksi Applen sertifikaatteja ei luoda eikä käydä läpi, miten iOS-laitteen rekisteröinti tehdään.

MobiControllin käyttöönotto tapahtuu lisäämällä käyttäjäagentit älypuhelimiin ja rekisteröimällä ne tuotantopalvelimelle. Tuotantopalvelimen WWW-hallintapaneelin kautta luodaan säännöt, joiden mukaan älypuhelimet lisätään hallittavaksi tuotantopalvelimeen. Tämän jälkeen asetetaan erilaiset käyttäjäprofiilit älypuhelimille rajoituksineen. MobiControllissa hallitaan älypuhelimia omien ryhmien mukaan. Käyttöönottoa varten älypuhelimet jaetaan kahteen ryhmään: VSHHP ja OptiScan-ryhmiin. Windows-laitteille luodaan Lightweight Directory Access Protokollaa (LDAP) käyttävä yhteys VSSHP:n AD-palvelimeen.

4.1 Vaatimukset ja asennus

SOTI MobiControllin asennukseen vaaditaan Windows-palvelinympäristö ja Microsoftin kehittämä .NET 4.5 -sovelluskehys. Tuotantopalvelimena käytetään Windows Server 2012R2 ja palvelimelle asennetaan MobiControllia vaatima tietokantapalvelin. Palvelimella oli etukäteen jo asennettuna SQL 2012-tietokanta palvelin ja näin ollen MobiControl tunnisti automaattisesti tietokantapalvelimen.

Windows-palvelimelle asetetaan julkinen IP-osoite, sillä palvelimen luontihetkellä palvelimella oli vain yksityinen IP-osoite. Julkisen IP-osoitteen ohella palomuurista avataan portit 5494, 5495, 636 ja 443 saapuvaa liikennettä varten. Porttien avaamisen jälkeen älypuhelimiin saa asennettua Device Agent (DA)

tuotantopalvelimeen yhteyden. DA saa yhteyden tuotantopalvelimeen portin 443 kautta SSL-salatulla HTTPS-yhteydellä.

MobiControllin DA:n on saatava yhteys ulkoverkosta tuotantopalvelimeen, jonka vuoksi avataan palomuurista portti 443 HTTPS-yhteyksiä varten. Tietoturvallisuuden vuoksi on asetettu, että Web-Console kuuntelee vain portilta 443 tulevia pyyntöjä, eli HTTPS-kutsuja. DA:n tulee olla versio 12.0.0 tai uudempi, jotta älypuhelimien rekisteröinti onnistuu tuotantopalvelimelle.

4.2 Älypuhelimien rekisteröiminen

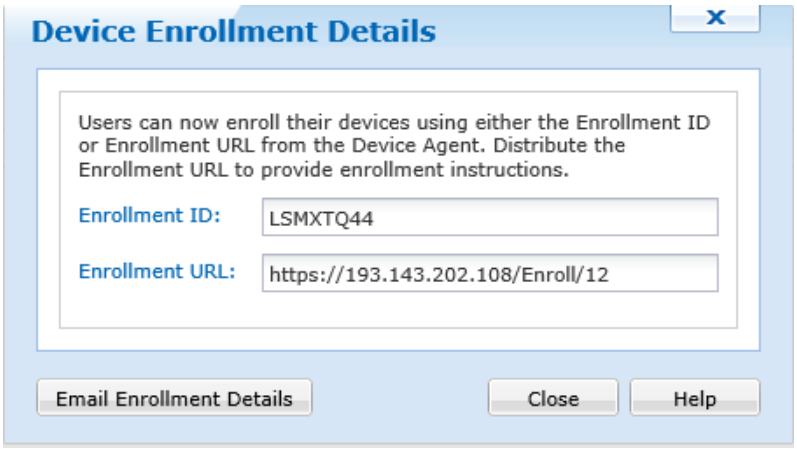
Laitteiden rekisteröinti tarkoittaa, että saadaan älypuhelimet rekisteröityä tuotantopalvelimen hallintajärjestelmään. MobiControl käyttää sääntöjä yksinkertaistaakseen toimintoja, joiden avulla hallitaan ja rekisteröidään älypuhelimia.

Ennen rekisteröintiä Web Consolessa luodaan säännöt, joiden mukaan rekisteröinti tehdään. Säännöt luodaan aina omalle käyttöliittymän omaavalle älypuhelimelle. Sääntöjen luontia laitekohtaisille älypuhelimille käydään tarkemmin seuraavissa alaluvuissa läpi.

4.2.1 Android-älypuhelimen rekisteröiminen

Android-laitteiden rekisteröinti suoritetaan luomalla sääntö, jonka mukaan laitteet tullaan rekisteröimään hallintojärjestelmään ja DA:n asentamiseksi. Web Consolesta luodaan uusi sääntö ja ensin luodaan nimi, jonka mukaan sääntö tehdään. Tässä kohtaa nimetään sääntö ”Medbit”, sillä päätelaitteet tulevat olemaan Medbitin käytössä. Android laitteiden rekisteröintiä varten voidaan päättää joko manuaalinen rekisteröinti tai LDAP-yhteyden avulla tehty rekisteröinti. Android-laitteiden yhteydessä valitaan manuaalinen rekisteröityminen, sillä kaikilla päätelaitteiden käyttäjillä ei välttämättä ole tunnuksia tehtynä VSSHP Active Directoryyn. DA:n lopullinen lataus tapahtuu Googlen omasta Play-kaupasta.

Lopuksi MobiControl luo koosteen tehdystä säännöstä ja tarkat ohjeet, mihin IP-osoitteeseen pitää mennä sekä tarvittavan Enrollment ID:n. (Kuva 9)

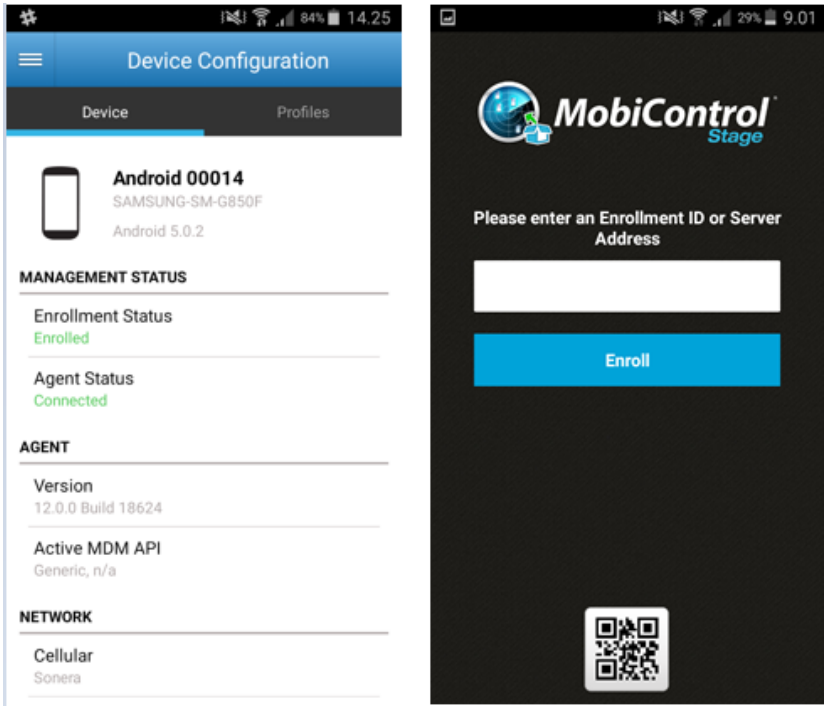


Kuva 9. Kooste säännön tekemisestä

Säännön luotua siirrytään annettuun WWW-osoitteeseen ja suoritetaan rekisteröinti loppuun. Tässä kohtaa tuotantopalvelimelle rekisteröiminen onnistuu julkisen IP-osoitteen kautta. Osoitteeseen siirrettyä pyydetään valitsemaan, mikä DA:n versio älypuhelimeen ladataan. SOTI on tehnyt lähes jokaiselle älypuhelinmallille oman DA:n, mutta tämän rekisteröimisen yhteydessä käytetään yleistä DA:ta, joka käy mille tahansa Android-laitteelle. (Kuva 10)

Kuva 10. Tuotantopalvelimelta valitaan millainen DA asennetaan älypuhelimeen.

Rekisteröiminen suoritetaan loppuun asettamalla joko tuotantopalvelimen URL-osoite tai reksiteröinti ID:n MobiControllin Device Agent Stage-ohjelmistoon, joka ladattiin Play-kaupasta. Tämän jälkeen älypuhelinta voidaan hallita Web Consolen kautta ja rekisteröityminen on suoritettu onnistuneesti (Kuva 11.)



Kuva 11. Laitteen onnistunut rekisteröiminen ja viimeistely

4.2.2 Windows älypuhelimen rekisteröinti

Windows-pohjaisten älypuhelimien rekisteröinti tapahtuu käyttämällä yrityksen Active Directorya säännön luomisessa. Windows-älypuhelimien rekisteröinnissä pitää käyttää Lightweight Directory Access Protokollaa (LDAP) onnistunutta rekisteröintiä varten. Säännön luomisen yhteydessä luodaan LDAP-yhteys yrityksen AD-palvelimelle HTTPS:n kanssa portin 636 kautta.

Ennen LDAP-yhteyden luomista otetaan selville, mihin AD-ryhmään ”users” kuuluu (Kuva 12). Oletusasetuksena on, että kaikki työntekijät VSSHP:ssa ja Medbitissä kuuluvat AD-ryhmään ”users” ja säännön luomisen yhteydessä pitää asettaa, mistä AD-ryhmästä rekisteröityminen hyväksytään.

```
C:\Users\KORGANJ_ADM>dsquery group -name users
"CN=Users,CN=Builtin,DC=vsshp,DC=net"
```

Kuva 12 AD-palvelimen dsqueryn tulokset ryhmätlä users

LDAP-yhteyden luonnin jälkeen asetetaan AD-ryhmät, joista käyttäjät voivat rekisteröidä oman Windows-puhelimensa. Asetetaan AD-ryhmäksi ”users” sekä ”Exchange Users” näin taaten, että kaikki, joilla on tunnukset VSSHP:n AD:ssä, saavat ladattua omaan puhelimeensa DA:n. Säännön luonnin yhteydessä MobiControl estää automaattisesti kaikista muista AD-ryhmistä tulevat kutsut. (Kuva 13.)

Info

Name	Value
Type	Add Devices Rule
Name	medbitTesti
Status	Enabled
Activate Date	2015-10-13 1:36:00 PM
Wildcard Filter Parameters	
Add Devices Rule Tag = "6E9A7F4C-0CA1-409E-0C91-98518770DF33"	
User Authentication Options	Utilize User Directory credentials
LDAP Connection	LDAP yhteys
Device Name	WindowsPhone %AUTONUM%
LDAP Mappings	
Kaikki Exchangen käyttäjät	VSSHP
Users	Medbit
Everyone Else	Deny Access
Default Rule	Yes
Preserve Device Location on Re-Enrollment	Yes
Certificate Authentication Authority	Internal MobiControl CA

Kuva 13. Windows-säännön yhteenveto.

Jotta Windows-puhelin voitiin lisätä tuotantopalvelimelle, käytettiin Windows 8.1 ominaisuutta asettamalla puhelimelle työpaikkatili. Työpaikkatilin asettamisen myötä älypuhelin tunnisti automaattisesti MobiControllin tuotantopalvelimen.

Windows-laitteiden rekisteröinti ei onnistunut, sillä ulkoisesta Internetistä ei saatu muodostettua LDAP-yhteyttä VSSHP:n AD-palvelimeen onnistuneesti, tiukkojen palomuuriasetusten takia. Windows-laitteiden rekisteröinti olisi onnistunut vain avaamalla AD-palvelimelta yhteyden ulkoverkkoon portin 443 kautta. Turvallisuussyistä näin ei tehty.

4.3 Älypuhelimen hallinta

Älypuhelimen hallintaa suoritetaan suoraan Web Consolen kautta. Älypuhelimia hallitaan tarkastelemalla, millaisia sovelluksia älypuhelimeen on asennettu, paikantamisella, jäljittämisellä, laitteen lukitsemisella ja tehdasasetuksien palauttamisella. Tämän lisäksi luodaan käyttäjäprofiileja, joiden avulla asetetaan erilaisia rajoitteita ja tuodaan asetuksia suoraan älypuhelimeen. Käyttäjäprofiilien luontia käydään läpi vain Android-pohjaisille laitteille seuraavassa luvussa.

4.4 Älypuhelimen rajoittaminen

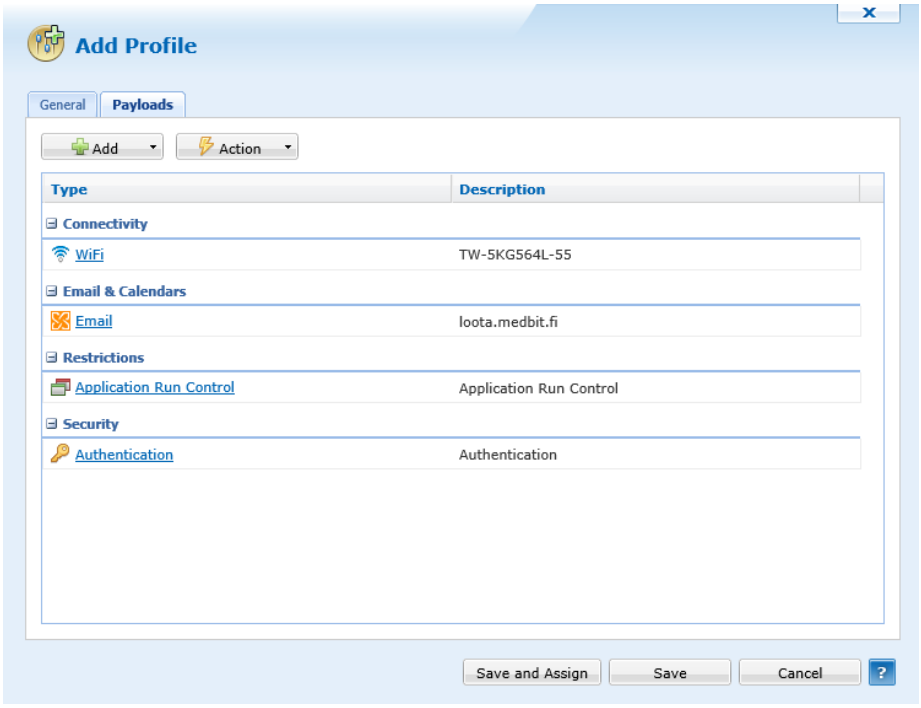
Jotta rajoitteita saadaan asetettua älypuhelimen käyttöön, luodaan hallintoryhmille erilaisia käyttäjäprofiileja. Käyttäjäprofiilit luodaan Medbitin vaatimusten mukaan ja rajataan, minne sivustoille voi mennä, mitä applikaatioita puhelimessa voidaan käyttää, ja konfiguroidaan sähköpostiasetukset. Käyttäjäprofiilien luonnin yhteydessä määritetään, mitä halutaan rajoittaa.

Ensin asetetaan rajoite, että Android-laitteilla ei saa käyttää seuraavia applikaatioita älypuhelimessa: Youtube, Internet Browser, GooglePlay. Lisäksi asetetaan rajoite, että käyttäjä ei pääse muuttamaan puhelimen omia asetuksia, ja estetään pääsy kaikille sivuille mainosten linkkien kautta. Tämän lisäksi lisätään käyttäjäprofiiliin jo valmiiksi Medbitin käyttämän Wifi-verkon asetukset. (Kuva 14.)

Turvallisuuden lisäämiseksi laitteelle asetetaan salasana. Jos salasanan kirjoittaa 10 kertaa väärin, MobiControl palauttaa laitteen tehdasasetuksiin.

Käyttäjäprofiilin luonnin jälkeen asetetaan profiilit kaikille älypuhelimille, jotka on onnistuneesti lisätty MobiControllin tuotantopalvelimeen. Käyttäjäprofiili asentuu automaattisesti kaikille laitteille, joille se asetetaan Web Consolen kautta.

Käyttäjäprofiileja voidaan luoda niin paljon kuin halutaan ja asettaa ne mille ryhmälle tahansa MobiControllissa. Medbitin tapauksessa yksi käyttäjäprofiili sopii hyvin kaikkiin laitteisiin, sillä vielä tällä hetkellä ei ole paljon laitteita, joita halutaan hallita.



Kuva 14. Käyttäjäprofiilin luonti ja rajoitteiden asettaminen

4.5 Sovelluksien asentaminen älypuhelimeen

Ensin MobiControllissa luodaan sääntö, jonka mukaan sovellusten asentaminen tapahtuu älypuhelimeen. Säännön luomisen yhteydessä saa päättää mistä sovelluksen saa ladattua. MobiControl tarjoaa kolme eri vaihtoehtoa: Google Play -kaupasta, Amazonin -sovellus kaupasta tai tuoda oma yrityksen kehittämä sovellus. Tähän vaiheeseen tuodaan tarvittavat sovellukset suoraan Google Play -kaupasta.

Sääntö luodaan Android älypuhelimille, ja aluksi asennetaan yksi sovellus älypuhelimille: viivakoodinlukija. Myöhemmin laitteille asennetaan yrityksen omia sovelluksia, mutta tässä vaiheessa niitä ei vielä ollut. Säännön luonnin jälkeen sovelluksen voi asentaa suoraan MobiControllin kautta.

5 YHTEENVETO

Opinnäytetyön tavoitteena oli testata ja käyttöönotattaa SOTI MobiControl MDM-palvelu, jonka avulla hallitaan älypuhelimia Medbit Oy:n sisällä sekä muissa projekteissa. Käyttöönoton yhteydessä piti varmistaa, että älypuhelimien hallinta ja rekisteröinti onnistuvat turvallisesti sekä yksinkertaisesti WWW-hallintapaneelin kautta. Tämän lisäksi piti luoda turvallinen verkkoympäristö käytössä olevalle Windows 2012R2 -tuotantopalvelimelle ja onnistuneesti rekisteröidä Android- sekä Windows-pohjaisia älypuhelimia MobiControlliin ulkoisesta verkosta. Käyttöönottoa varten tuli olla hyvä tietämys verkkoturvallisuudesta, Windows-palvelimista ja porttien toiminnollisuudesta.

Opinnäytetyön teoriaosuudessa käytiin läpi, miten luodaan turvallinen verkkoympäristö yrityksen käyttöön ja mitä erilaisia menetelmiä voidaan käyttää, jotta voidaan tehostaa turvallisuutta vielä enemmän. Tämän pohjalta luotiin turvallinen verkkoympäristö tuotantopalvelinta varten. Opinnäytetyön aikana Android-pohjaiset älypuhelimet saatiin rekisteröityä hallintajärjestelmään onnistuneesti, mutta Windows-pohjaisten älypuhelimien rekisteröiminen ei onnistunut tiukoista palomuurikäytännöistä ja asetuksien takia.

Opinnäytetyön aikana ongelmia tuottivat mm. VSSHP:n verkko, vanhentuneet ohjeet, joita SOTI tarjosi tuotteestaan, ja LDAP-yhteyden saaminen Active Directory -palvelimeen. Palvelin sijaitsi VSSHP:n verkossa, ja näin ollen yhteyden luominen ulkoverkosta oli hankalaa palomuuriasetuksien vuoksi. Koska dokumentaatiota ei ollut saatavilla, minkä vuoksi LDAP-yhteydenkin luominen osoittautui aluksi hankalaksi. Tämän lisäksi virheilmoitukset palauttivat vain tiedon ”Enrollment failed” eikä sen tarkempaa tietoa saanut. Usein joutui ottamaan yhteyttä SOTI:n tekniseen tukeen, jotta sai tiedon, miten tietyt toiminnot, kuten käyttäjäprofiilit, toimivat.

Opinnäytetyön aikana vaatimukset ja tavoitteet pysyivät samoina, minkä vuoksi käyttöönotto ei viivästynyt aikataulusta. Käyttöönotossa ei ollut ylitsepääsemättömiä ongelmia, ja MobiControllin perustoiminnot sekä hallitsemisominaisuudet

toimivat moitteettomasti. Hallintapaneelin käytön opettamiseen vaaditaan vain yksinkertaiset ohjeet, minkä vuoksi MobiControl oli tuotteena sopiva Medbit Oy:lle.

MDM-ratkaisua halutaan soveltaa jo muihinkin projekteihin Medbit Oy:n sisällä. SOTI MobiControllin ratkaisun ja tuotantopalvelimen asetuksien myötä saadaan onnistuneesti rekisteröityä Android-laitteita MobiControllin hallintajärjestelmään ulkoverkosta. Tämän ominaisuuden vuoksi MDM-ratkaisuja halutaan käyttää myös muissa projekteissa, sillä ennen on jouduttu käyttämään sovelluksia, jotka ovat toimineet ainoastaan VSSHP:n sisäverkossa.

LÄHTEET

Boyle, R. & Panko, R. 2012. Corporate Computer Security. 3. painos. New Jersey: Prentice Hall.

Brody H 2013. How HTTPS Secures Connections: What Every Web Dev Should Know. Viitattu 14.10.2015. https://blog.hartleybrody.com/https-certificates/

Definition of: port Forwarding. “Definition of: port Forwarding.”. Viitattu 7.10.2015 http://www.pcmag.com/encyclopedia/term/49509/port-forwarding

Digicert 2015. What is SSL (Secure Sockets Layer) and What Are SSL Certificates? Viitattu 10.10.2015 https://www.digicert.com/ssl.htm

Dye, M & McDonald, R & Rufi, A 2008. Network Fundamentals, CCNA Exploration Companion Guide. Indianapolis: Cisco Press.

Ellis, L & Saret, J & Weed, P 2012. BYOD: From company-issued to employee-owned devices. McKin-sey&Company.http://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/High%20Tech/PDFs/BYOD_means_so_long_to_company-issued_devices_March_2012.ashx

Bagheri, E 2013. Evolution of Mobile Device Management Tools And Analysing Integration Models For Mobility Enterprise. Sweden: Umeå University

Horman, S 2005. SSL and TLS An Overview of A Secure Communications Protocol. Viitattu 11.10.2015 http://horms.net/projects/ssl_and_tls/stuff/ssl_and_tls.pdf

Kangas, E 2008. SSL versus TLS – What’s the difference? Viitattu 11.10.2015. https://luxsci.com/blog/ssl-versus-tls-whats-the-difference.html

Medbit Oy 2015. Terveitä Ratkaisuja. Viitattu 7.10.2015 www.medbit.eu/yritys/

Microsoft 2005. Data Confidentiality. Viitattu 11.10.2015 https://msdn.microsoft.com/en-us/library/ff650720.aspx

Mobility Solutions 2015. SOTI MobiControl v12. Viitattu 16.10.2015 http://www.mobilitysolutions.cz/eng/news/299-soti-mobicontrol-v12

Networking Basics 2015. ”Networking Basics”. Viitattu 8.10.2015 http://www.networking-basics.net/)

Pinzon, S 2015. What Is A Port (and Why Should I Block It?) Viitattu 8.10.2015 http://www.watchguard.com/wgrd-resource-center/security-fundamentals/what-is-a-port

RTFM 2000. http Over TLS. Viitattu 13.10.2015. http://www.ietf.org/rfc/rfc2818.txt.

SOTI 2013. MobiControl Administration Utility. Viitattu 15.10 https://www.soti.net/mc/help/v11/en/Content/Setup/MCAU.htm

SOTI 2015a. SOTI MobiControl. Viitattu 15.10.2015 https://www.soti.net/mobicontrol/

SOTI 2015b. MobiControl Features. Viitattu 15.10.2015 https://www.soti.net/mobicontrol/key-features/

SOTI 2015c. MobiControl Help PDF. Viitattu 16.10.2015 https://www.soti.net/PDF/MCHelp.pdf

SOTI 2015d. All Devices Tab. Viitattu 17.10.2015 http://www.soti.net/mc/help/v9.03/en/Content/Web/Devices/AllDevices.htm

TechRepublic Shinder, D 2005. SolutionBase: Strengthen Network defenses by using a DMZ. Viitattu 14.10.2015 http://www.techrepublic.com/article/solutionbase-strengthen-network-defenses-by-using-a-dmz/

TechTarget 2013. Mobile device management (MDM) definition. Viitattu 6.10.2015 http://searchmobilecomputing.techtarget.com/definition/mobile-device-management