Opinnäytetyö (AMK)

Tietojenkäsittely

Tietoliikenne

2014

Jussi Berg

MOBIILILAITTEIDEN HALLINTAJÄRJESTELMÄN TESTAUS

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Tietoliikenne

Elokuu 2014 | 66 sivua

Esko Vainikka

Jussi Berg

MOBIILILAITTEIDEN HALLINTAJÄRJESTELMÄN TESTAUS

Tämän opinnäytetyön tavoitteena oli suorittaa käytännön testausprosessi mobiililaitteiden hallintajärjestelmälle. Hallintajärjestelmän testaus tehtiin toimeksiantona teknologiayritys Telestelle. Testattava hallintajärjestelmä oli Symantecin Mobile Management. Hallintajärjestelmän testauksella haluttiin selvittää uuden käyttöönotettavan järjestelmän toimintavarmuus, toimintaperiaate, ominaisuudet ja yhteensopivuus kohdelaitteiden kanssa. Tärkein yksittäinen päämäärä testauksessa oli selvittää, onko hallintajärjestelmässä jokin sellainen ongelma, joka voisi estää järjestelmän lopullisen implementoinnin.

Työn teoriaosuudessa perehdytään mobiililaitteisiin, niiden käyttöjärjestelmiin, turvallisen laitehallinnan menetelmiin sekä mobiililaitteisiin kohdistuviin uhkiin.

Työn empiirinen osuus koostuu hallintajärjestelmän testaussuunnitelmasta, testattavien ominaisuuksien kuvailusta sekä itse testausprosessin tuloksista. Testaussuunnitelmassa käsitellään testauksen alkuasetelma ja tavoitteet, hallintajärjestelmän kuvaus, testausympäristö ja laitteet sekä testausmenetelmät.

Opinnäytetyön johtopäätöksissä arvioidaan testauksen tuloksia ja pohditaan, onko hallintajärjestelmä valmis implementoitavaksi.

ASIASANAT:

Symantec, mobiililaite, hallintajärjestelmä, laitehallinta, etähallinta, testaus

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Data Communications

August 2014 | 66 pages

Esko Vainikka

Jussi Berg

TESTING OF MOBILE DEVICE MANAGEMENT SYSTEM

The aim of this thesis was to conduct a testing process for a mobile device management system. The testing of the mobile device management was commissioned by Teleste, a technology company. The system being tested was Symantec Mobile Management. The goal of the test process was to study the reliability, the operating principle, features and compatibility of the new mobile device management system. The single most important goal of the testing was to determine whether the management system had any kind of fatal problem that could prevent the system from being implemented for official use in the company.

The theoretical part of the thesis discusses the characteristics of mobile devices, their operating systems, the methods for secure device management and threats that mobile devices face.

The empirical part of the thesis introduces the test plan for MDM system, describes the characteristics of the tested MDM abilities, as well as the results of the testing process. The test plan discusses the objectives of the testing, the overview of the MDM system, the test environment, equipment used in the testing and the methods used in the testing process.

The conclusion section of the thesis analyzes the test results and discusses whether the management system is ready to be implemented.

KEYWORDS:

Symantec, mobile device, MDM, device management, remote control, testing

SISÄLTÖ

LIITTEET

KUVAT

TAULUKOT

1 JOHDANTO

Nykypäivän älykkäät mobiililaitteet ovat jo monen vuoden ajan saavuttaneet perinteisiä tietokoneita niin ominaisuuksiltaan kuin suorituskyvyltään. Mobiililaitteilla voidaan tehdä jo monia samoja työtehtäviä kuin perinteisillä pöytä- tai kannettavilla tietokoneilla. Tämä luo uusia haasteita tietoturvan, tiedonvarmistamisen ja tiedon suojaamisen osa-alueilla. Näihin haasteisiin voidaan vastata mobiililaitteiden hallintajärjestelmällä.

Keskitetyllä mobiililaitehallinnalla pyritään parantamaan tietoturvaa ja virtaviivaistamaan sekä yhtenäistämään yrityksen omistamien laitteiden hallintaa. Hallintajärjestelmän ominaisuuksiin kuuluu tyypillisesti esimerkiksi datan, applikaatioiden ja hallintakomentojen jakaminen etäyhteyden avulla.

Tämän opinnäytetyön tavoitteena oli suorittaa käytännön testausprosessi mobiililaitteiden hallintajärjestelmälle. Hallintajärjestelmän testaus suoritettiin toimeksiantona Telestelle. Teleste on kansainvälinen teknologiakonserni, joka kehittää ja tarjoaa video- ja laajakaista -teknologioita ja niihin liittyviä palveluita. Liiketoiminta on jaettu kahteen liiketoiminta-alueeseen: Video and Broadband Solutions ja Network Services. (Teleste 2013.)

Hallintajärjestelmän testauksella haluttiin selvittää uuden käyttöönotettavan järjestelmän toimintavarmuus, toimintaperiaate, ominaisuudet ja yhteensopivuus kohdelaitteiden kanssa. Toimeksiantoyrityksellä oli jo ennestään käytössä mobiililaitteiden hallintajärjestelmä. Uusi hallintajärjestelmä oli kuitenkin eri toimittajalta, joten järjestelmän testaus oli tarpeen ennen sen lopullista implementointia.

Opinnäytetyön teoriaosuudessa haluttiin myös käsitellä laitehallintaan läheisesti liittyviä muita osa-alueita. Teoriaosuudessa käsitellään mobiililaitteiden ominaisuudet, käyttöjärjestelmien määrittely, menetelmät turvalliseen laitehallintaan, laite- ja tietoturvapolitiikkaa sekä mobiililaitteisiin kohdistuvia uhkia. Nämä aihealueet ovat tärkeitä, koska usein juuri keskitetyllä laitehallinnalla voidaan torjua tietoturvauhkia sekä asettaa haluttuja käyttöpolitiikka-asetuksia kohdelaitteisiin.

2 MOBIILILAITTEIDEN MÄÄRITTÄMINEN

Keskitetyn hallintajärjestelmän testausprosessin kannalta on tärkeää määrittää tietyt mobiililaitteiden ominaispiirteet. Tähän prosessiin kuuluu olennaisena osana itse laitteiden sekä laitteiden käyttöjärjestelmien ominaisuuksien määrittäminen.

Mobiililaitteen käyttöjärjestelmä määrittää tietyiltä osin, mitä keskitetyn hallintajärjestelmän tarjoamia ominaisuuksia voidaan yksittäiseen laitteeseen kohdistaa. Nämä seikat on otettu huomioon keskitetyn hallintajärjestelmän testauksessa.

2.1 Käyttöjärjestelmän määrittely

Mobiilikäyttöjärjestelmä on ohjelmisto, joka on suunniteltu käytettäväksi älypuhelimissa, tableteissa, kämmentietokoneissa (PDA) sekä ns. perinteisissä matkapuhelimissa.

Älypuhelimet ja tabletit käyttävät usein moderneja mobiililaitteisiin tarkoitettuja käyttöjärjestelmiä. Modernit mobiilikäyttöjärjestelmät tarjoavat perinteisten viestintä- ja puheominaisuuksien lisäksi ominaisuuksia, jotka ovat tuttuja tietokoneiden käyttöjärjestelmistä. Modernit mobiilikäyttöjärjestelmät tarjoavat käyttäjälle kattavat ominaisuudet, kuten sähköpostin, pikaviestiominaisuudet, sovellusten moniajon ja laajat multimediaominaisuudet. Älypuhelinten ja tablettien modernit käyttöjärjestelmät ovat myös mahdollistaneet applikaatioiden lataamisen sovelluskaupoista. Applikaatiosta käytetään myös perinteistä termiä sovellus. Applikaatio voi esimerkiksi olla älypuhelimeen ladattava herätyskello tai pikaviestin.

Mobiililaitteissa käyttöjärjestelmä on suunniteltu ottaen huomioon laitteiden ominaisuudet sekä rajoittavat tekijät. Usein älypuhelimissa ja tableissa on esimerkiksi rajatusti käyttömuistia, pienehkö näytön koko, käyttöliittymä on kosketuspohjainen ja käyttöjärjestelmä täytyy suunnitella laitteen akun kannalta ener-

giatehokkaaksi. Tällaiset rajoitteet luovat usein tilanteen, jossa tietokoneiden käyttöjärjestelmiä ei voida suoraan käyttää mobiililaitteissa.

2.2 Mobiililaitteiden käyttöjärjestelmät

Keskitetyn hallintajärjestelmän ominaisuuksia ja käyttötapauksia testattiin usealla eri mobiililaitteella, jotka käyttivät useita eri käyttöjärjestelmiä. Käyttöjärjestelmä määrittää osittain, mitä ominaisuuksia hallintajärjestelmä tarjoaa kyseiselle käyttöjärjestelmälle. Tämän takia on tärkeää määrittää tietyt perusasiat testauksessa käytettävistä käyttöjärjestelmistä.

2.2.1 Apple iOS

Applen kehittämä iOS-käyttöjärjestelmä löytyy useista eri Applen valmistamista laitteista, kuten iPhone, iPad, iPod ja Apple TV. Apple hallinnoi voimakkaasti käyttöjärjestelmää ja sen kehitystä, tämän takia iOS-käyttöjärjestelmä toimii vain Applen valmistamissa laitteissa. Apple ei ole sallinut iOS-käyttöjärjestelmän hyödyntämistä kolmannen osapuolen laitteissa. Applen iOS-käyttöjärjestelmä lanseerattiin iPhone-älypuhelimen käyttöjärjestelmänä. Se oli ilmestyessään moderni käyttöjärjestelmä ja aloitti laitemarkkinoilla nykyaikaisten älykkäiden mobiililaitteiden vallankumouksen. (Campagna ym. 2011, 32.)

iOS perustuu Applen Mac OS X -käyttöjärjestelmään, jota käytetään Applen valmistamissa pöytä- ja kannettavissa tietokoneissa. Kuten muutkin mobiilikäyttöjärjestelmät, iOS sisältää ohjelmistokehittäjän työkalut eli SDK:n, jonka avulla kolmannet osapuolet voivat kehittää ja jakaa applikaatioita iOS-pohjaisille laitteille. (Campagna ym. 2011, 32.)

Applikaatioita iOS-käyttöjärjestelmälle pystyy lataamaan virallisesta Applen sovelluskaupasta eli App Storesta, josta lokakuussa 2013 löytyi jo yli miljoona applikaatiota (Ingraham 2013).

Apple kontrolloi tiukasti iOS-käyttöjärjestelmän laitteistoa sekä asennettuja applikaatioita, mikä on tietoturvan näkökulmasta kaksijakoinen käytäntö.

Positiivisena asiana voidaan pitää esimerkiksi sitä, että Apple pystyy seulomaan App Store -sovelluskauppaan julkaistavat applikaatiot tehokkaammin haittaohjelmien varalta. Tiukalla kontrollilla Apple voi esimerkiksi hallita paremmin applikaatioiden tarvitsemia käyttöoikeuksia ja laiteominaisuuksia. Applen filosofian mukaan käyttöjärjestelmän suljettu lähdekoodi ja tiukka kontrolli ovat toimivia keinoja haittaohjelmien ja haavoittuvuuksien torjuntaan. (Campagna ym. 2011, 32.)

Tiukan kontrollin haittapuolena voidaan pitää esimerkiksi sitä, että Apple on tietoisesti rajoittanut kolmansien osapuolten tietoturva-applikaatioiden, kuten perinteisen virustorjunnan, julkaisemista iOS-alustalle (Campagna ym. 2011, 33).

Yrityksissä tiukan kontrollin rajoitteet voivat tietyiltä osin heikentää IT-järjestelmävalvojan keinoja ylläpitää toimivaa tietoturvallista käyttöympäristöä. iOS-käyttöjärjestelmän hallinnassa on syytä ottaa huomioon jailbreakin mahdollisuus. Jailbreak on prosessi, jossa Applen mobiilialustalleen asettamat rajoitukset poistetaan halutusta kohdelaitteesta.

2.2.2 Google Android

Android on Googlen kehittämä avoimen lähdekoodin käyttöjärjestelmä, joka pohjautuu Linux-käyttöjärjestelmään. Android-pohjaisiin laitteisiin applikaatioita voi ladata esimerkiksi Googlen omasta virallisesta Google Play -sovelluskaupasta. Googlen Androidille on ladattavissa yli miljoona applikaatiota sovelluskaupasta (Appbrain 2014).

Avoimen lähdekoodin Android antaa laitevalmistajille tietyissä ominaisuuksissa vapaat kädet toteuttaa omia ratkaisujaan, esimerkkinä räätälöity graafinen käyttöliittymä. Google kuitenkin määrittelee laitevalmistajille tietyt ohjesäännöt Androidin käytölle.

Avoimen lähdekoodin käyttöjärjestelmä on tietoturvan näkökulmasta erilaisessa asemassa verrattuna suljetun lähdekoodin käyttöjärjestelmiin.

Avoin lähdekoodi tarkoittaa käytännössä sitä, että lähdekoodi on kaikkien halukkaiden luettavissa ja vapaasti muokattavissa. Android-käyttöjärjestelmän avoin lähdekoodi saattaa altistaa sille, että järjestelmän eri versioista on helpompi löytää haavoittuvuuksia. Toisaalta avoimen lähdekoodin luonne merkitsee myös sitä, että suuri kehittäjäyhteisö seuraa käyttöjärjestelmän kehitystä ja lähdekoodia tarkasti (Campagna ym. 2011, 35). Avoimesta lähdekoodista mahdolliset haavoittuvuudet voidaan havaita ja korjata nopeasti.

Koska Android on avoimen lähdekoodin käyttöjärjestelmä, on siitä luotu useita epävirallisia variantteja ja jakeluita, esimerkiksi Cyanogenmod-jakeluversio. Nämä epäviralliset jakeluversiot vaativat aina kohdelaitteen roottaamisen. Roottaminen on prosessi, jolla murretaan puhelimen suojaukset, jotta saadaan käyttöön pääkäyttäjän eli ns. Root-käyttäjän oikeudet.

2.2.3 Microsoft Windows Mobile ja Windows Phone

Windows Mobile ja Windows Phone ovat Microsoftin kehittämiä suljetun lähdekoodin mobiilikäyttöjärjestelmiä. Windows Mobile -käyttöjärjestelmä oli vahvasti suunniteltu yritysmaailman käyttötarpeisiin ja siksi markkinoilla oli vain pieni määrä Windows Mobileen perustuvia kuluttajalaitteita. Windows Mobilen vahva suuntautuminen yritysmarkkinoille merkitsi sitä, että se sisälsi useita sisäänrakennettuja tietoturvaominaisuuksia sekä laajat rajapinnat kehitystyölle. Näiden ominaisuuksien avulla kehittäjät pystyivät luomaan kolmannen osapuolen tietoturvasovelluksia sekä laitteiden hallintajärjestelmiä. (Campagna ym. 2011, 36.)

Käytännössä Microsoftin tuoreempi Windows Phone -käyttöjärjestelmä on korvannut täysin jo vanhentuneen Windows Mobile -käyttöjärjestelmän (Campagna ym. 2011, 36). Laitevalmistajat eivät enää tuo markkinoille laitteita, joissa käytetään Windows Mobile -käyttöjärjestelmää.

Windows Phonen ensimmäinen virallinen versionumero oli 7. Nimeämiskäytäntö oli osittain harhaanjohtava, koska Windows Phone 7 oli täysin uusi käyttöjärjestelmä ja se erosi huomattavasti aiemmasta Windows Mobile -käyttöjärjestelmästä, jonka viimeiseksi kehitysversioksi jäi versionumero 6.5. (Campagna ym. 2011, 36.)

Windows Phone 7:stä puuttui kuitenkin useita yritysten tietoturvalle tärkeitä ominaisuuksia, kuten kattava VPN-tuki ja tietyt mobiililaitteen salausominaisuudet (Campagna ym. 2011, 36). Windows Phone -käyttöjärjestelmän tuoreemmat kehitysversiot ovat kuitenkin tuoneet mukanaan kaivattuja ominaisuuksia, kuten sisäänrakennetun VPN-tuen (Gruman 2014). Kirjoittamisen hetkellä Windows Phone -käyttöjärjestelmän uusin versionumero on 8.1.

2.2.4 Symbian

Symbian on avoimen lähdekoodin käyttöjärjestelmä, jota on pääsääntöisesti käytetty Nokian omissa mobiililaitteissa (Campagna ym. 2011, 37).

Symbianiin pohjautuvia variantteja on useita, esimerkiksi Series 60, Series 80 tai Symbian^3. Nämä käyttöjärjestelmän variantit eroavat toisistaan ominaisuuksiltaan sekä graafiselta ulkoasultaan.

Symbian on kuitenkin kuoleva käyttöjärjestelmä. Modernit älypuhelimet ja tabletit ovat siirtyneet kehittyneempiin käyttöjärjestelmiin, kuten Googlen Androidiin tai Applen iOS:ään (Campagna ym. 2011, 37).

Monissa yrityksissä saattaa vielä kuitenkin olla mobiililaitteita, jotka käyttävät Symbiania. Useimmat keskitetyt hallintajärjestelmät kuitenkin yhä tukevat Symbian-käyttöjärjestelmää Microsoft Exchangen ActiveSyncin kautta ja tarjoavat tälle käyttöjärjestelmälle vähintään perustason hallintaominaisuudet.

2.3 Mobiililaitteiden ominaispiirteet

Mobiililaitteisiin tulee luonnollisesti uusien kehityssukupolvien myötä myös uusia teknisiä innovaatioita ja ominaisuuksia. Näiden muutosten myötä laitteisiin kohdistuvat tietoturvauhat ja hyökkäysmenetelmät kehittyvät jatkuvasti. Laitteiden ominaispiirteet vaikuttavat myös suoraan siihen, minkälaisia ominaisuuksia mobiililaitehallinnan järjestelmät tarjoavat. Tämän takia on tärkeää määrittää mobiililaitteiden yleisimmät ominaispiirteet ja ominaisuudet.

Liikkuvuus

Mobiililaitteiden yksi kuvaavimmista ominaisuuksista on laitteiden liikkuvuus. Seuraavat ominaispiirteet mahdollistavat laitteiden liikkuvuuden:

- Mobiililaitteet ovat fyysisesti pienikokoisia ja painoltaan kevyitä.
- Nykyaikainen akkuteknologia mahdollistaa laitteiden pitkät valmiusajat.
- Älykkäät mobiililaitteet voivat tiedonsiirrossa tehokkaasti hyödyntää langattomia verkkoyhteyksiä.

Verkkoyhteydet

Älykkäissä mobiililaitteissa on vähintään yksi verkkorajapinta langattomia tietoliikenneyhteyksiä varten (Scarfone & Souppaya 2013, 2). Yleisin tapa muodostaa langaton verkkoyhteys on joko käyttää Wi-Fi -verkkoja tai hyödyntää puhelinoperaattoreiden tarjoamia datayhteyksiä, kuten 3G- tai 4G -verkkoja.

Mobiililaitteissa on myös muita ominaisuuksia, jotka hyödyntävät seuraavia verkkopohjaisia tekniikoita:

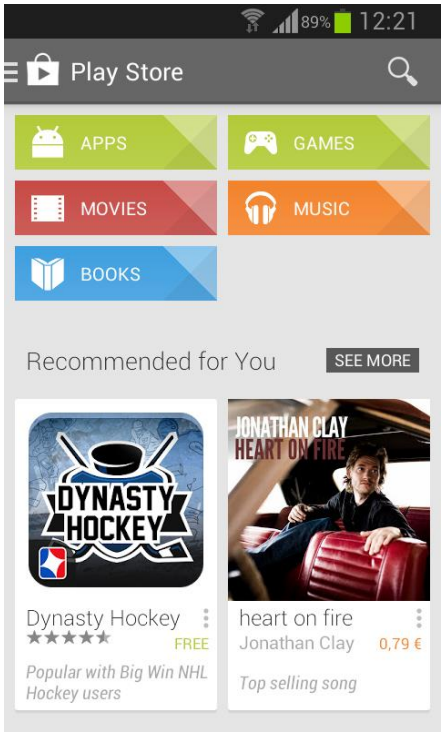
- Yksi tai useampi rajapinta, jotka mahdollistavat laitteen puheviestinnän, esimerkkinä perinteinen puhelinverkko.
- GPS-vastaanotin, jonka avulla voidaan hyödyntää esimerkiksi paikannuspalveluita.

- Yksi tai useampi lähikenttäviestinnän ja datasiirron mahdollistava rajapinta, esimerkkinä Bluetooth (Scarfone & Souppaya 2013, 2).

Applikaatiot

Älykkäässä mobiililaitteessa applikaatioita on saatavilla seuraavin keinoin:

- valmistajan laitteeseen valmiiksi asentamat applikaatiot
- laitteen käyttöjärjestelmän mukana tulevat applikaatiot
- virallisesta sovelluskaupasta ladattavat applikaatiot
- epävirallisesta sovelluskaupasta ladattavat applikaatiot.



Kuva 1. Näkymä Google Play -sovelluskaupan etusivusta.

Virallisista sovelluskaupoista, kuten Google Play (Kuva 1), laitteille on saatavissa sekä maksuttomia että maksullisia applikaatioita, pelejä, musiikkia sekä elektronisia kirjoja. Virallisten sovelluskauppojen eduksi voidaan yleensä laskea

kauppojen luotettavuus asiakkaiden näkökulmasta, sillä useimmissa sovelluskaupoissa ylläpitotaho tekee perustason tarkistuksen sovelluskauppaan ladatuille applikaatioille. Tarkistuksessa pyritään havaitsemaan mahdolliset haittaohjelmat sekä muut tietoturvauhat, jotka kohdistuvat käyttäjään. Virallisten sovelluskauppojen käytännöissä on kuitenkin eroja. Joissakin sovelluskaupoissa applikaatioihin kohdistuvat säännöt, vaatimukset ja tarkistukset saattavat olla merkittävästi tiukempia.

Applikaatioita on myös mahdollista ladata epävirallisista sovelluskaupoista, esimerkkinä Amazon Appstore. Yleensä hyvin tunnetuissa, epävirallisissa sovelluskaupoissa on hyvin samantyyppiset säännöt, vaatimukset ja tietoturvatarkastukset kuin virallisissa sovelluskaupoissa.

Epävirallinen sovelluskauppa voi kuitenkin olla uhka käyttäjän tietoturvalle. Joidenkin epävirallisten sovelluskauppojen kautta voidaan tahallisesti levittää haittaohjelmia saastuneiden applikaatioiden muodossa. Rehellisesti toimivissa epävirallisissa sovelluskaupoissa voi myös esiintyä haittaohjelmia. Jos yritys laiminlyö applikaatioiden tietoturvatarkastukset, on vaarana, että saastuneita applikaatioita päätyy sovelluskauppaan käyttäjien ladattavaksi.

Multimediaominaisuudet

Nykyaikaiset älykkäät mobiililaitteet sisältävät myös kattavat mediaominaisuudet. Laitteissa on useasti yksi tai useampi digitaalinen kamera, jonka avulla voidaan ottaa valokuvia tai videokuvaa. Laitteissa on myös aina oletusarvoisesti mikrofoni, jota käytetään puheviestinnässä tai esimerkiksi kaappaamaan ääntä videokuvaan. (Scarfone & Souppaya 2013, 2.)

Datan tallennus

Mobiililaitteissa on sisäinen kiinteä massamuisti, jota käytetään tallennustilana. Tallennustilan kapasiteettia voidaan kuitenkin usein laajentaa irrotettavalla tallennusmedialla, esimerkiksi SD-muistikortilla. Mobiililaitetta itseään voidaan

myös käyttää irrotettavana tallennusmediana jossain muussa laitteessa, kuten tietokoneessa (Scarfone & Souppaya 2013, 3).

Älykkäissä mobiililaitteissa on sisäänrakennettu tuki datan synkronoinnille. Data voidaan synkronoida joko langallisesti tai langattomasti. Dataa voidaan synkronoida kaksisuuntaisesti esimerkiksi perinteisten tietokoneiden, älypuhelimien, palvelimien ja pilvipalveluiden välillä. (Scarfone & Souppaya 2013, 3.) Synkronoitava data voi esimerkiksi olla kontaktitietoja, kalenterimerkintöjä, kuvia tai muita multimediatiedostoja.

3 MENETELMÄT TURVALLISEEN LAITEHALLINTAAN

Keskitetty mobiililaitteiden hallintajärjestelmä on nykypäivänä tehokas ratkaisu, kun yritys haluaa hallita suuria määriä työympäristössä käytettäviä mobiililaitteita. Hallintajärjestelmän eduiksi voidaan lukea esimerkiksi suurien laitemäärien helpompi käyttökontrolli, laiteasetusten konfigurointi, turvallisuuspolitiikan asettaminen laitteisiin ja mahdollisuus luoda turvallinen yhdyskäytävä laitteesta yrityksen tärkeisiin resursseihin.

Mobiililaitehallinnan tietoturvatavoitteet voidaan jakaa kolmeen pääryhmään:

- **Luottamuksellisuus**. Varmistetaan, että lähetetty tai vastaanotettu data on vain asianomaisten henkilöiden käytettävissä
- **Eheys**. Varmistetaan, että lähetettävä tai vastaanotettava data on sisäisesti eheää, eikä sitä ole tahallisesti tai tahattomasti muokattu
- **Saatavuus**. Varmistetaan, että käyttöoikeudet ovat oikeanlaiset ja että resurssit ovat saatavilla aina tarvittaessa (Intertek 2007).

Nämä tavoitteet voidaan saavuttaa toteuttamalla hyviä tietoturvakäytäntöjä mobiililaitehallinnassa.

Mobiililaitteiden hallintajärjestelmät voidaan jakaa kahteen erilaiseen toteuttamistapaan:

- käyttämällä viestipalvelimen sisäänrakennettuja ominaisuuksia mobiililaitteiden hallitsemiseen, esimerkkinä Microsoft Exchangen ActiveSync -ominaisuudet
- käyttämällä kolmannen osapuolen hallintajärjestelmää, jolla voidaan ohjata rinnakkain suuria määriä mobiililaitteita riippumatta siitä, mikä käyttöjärjestelmä kohdelaitteessa on (Scarfone & Souppaya 2013, 7).

Molemmat lähestymistavat tarjoavat tarvittavat perustason ominaisuudet laitehallintaan.

Yritykset voivat merkittävästi kehittää mobiililaitteidensa tietoturvaa ja hallintastrategiaa seuraavilla käytännöillä.

3.1 Yrityksen mobiililaitteiden tietoturvapolitiikka

Yrityksen tietoturvapolitiikassa on syytä määrittää, mihin yrityksen resursseihin mobiililaitteilla on pääsyoikeudet, onko kaikilla laitetyypeillä samanlaiset käyttöoikeudet ja millaiset resurssien käyttöoikeudet laitteille on ylipäätään myönnetty. Tietoturvapolitiikassa on myös syytä huomioida, onko BYOD-politiikan (selite kappaleessa 3.7) laitteilla samat käyttö- ja pääsyoikeudet kuin yrityksen omistamilla laitteilla (Scarfone & Souppaya 2013, vi).

Tietoturvapolitiikassa on toimivan laitehallinnan vuoksi määritettävä, kuka hallinnoi yrityksen mobiililaitehallinnan keskuspalvelimia, miten palvelimien käytäntöpolitiikkaa päivitetään sekä miten dokumentoidaan muut tarvittavat vaatimukset. Mobiililaitteiden tietoturvapolitiikka on myös syytä dokumentoida yrityksen yleisessä tietoturvasuunnitelmassa. Mobiililaitteiden tietoturvapolitiikka on pyrittävä suunnittelemaan niin, että se on mahdollisimman johdonmukainen ja yhtenevä yrityksen muun tietoturvapolitiikan kanssa. (Scarfone & Souppaya 2013, vi.)

3.2 Tarvittavien uhkamallien määrittäminen

Yrityksen tietoturvan kannalta on tärkeää määrittää uhkamallit mobiililaitteille. Laitteita käytetään sekä yrityksen omissa tiloissa, mutta myös yrityksen ulkopuolisessa ympäristössä. Mobiililaitteisiin kohdistuu tämän suuren liikkuvuuden takia usein enemmän tietoturvauhkia. (Scarfone & Souppaya 2013, vi-vii.)

Vertailukohteeksi voidaan ottaa esimerkiksi perinteiset pöytäkoneet, joita pääsääntöisesti käytetään yrityksen omissa tiloissa ja jotka käyttävät tietoliikenteeseen yrityksen omaa sisäverkkoa. Pöytäkoneisiin voidaan näin ollen kohdistaa vain tietynlaisia hyökkäysmenetelmiä.

Uhkamallien määrittäminen auttaa yritystä tunnistamaan tarvittavat vaatimukset toimivan tietoturvan kehittämiseksi. Uhkamallien perusteella voidaan myös tehdä tarvittavat muutokset keskitetyn hallintajärjestelmän politiikkaan ja asetuksiin, jotta yrityksen tietoturva saadaan halutulle tasolle.

Uhkamallien määrittelyyn kuuluu olennaisesti yrityksen tärkeiden resurssien tunnistaminen, niihin kohdistuvat mahdolliset uhat ja haavoittuvuudet sekä millaisia turvallisuuskäytäntöjä resursseissa sovelletaan. Kun uhat ja haavoittuvuudet on tiedostettu, arvioidaan hyökkäysten mahdollinen lukumäärä, hyökkäysten onnistumisen todennäköisyys sekä kuinka suurta vahinkoa hyökkäykset voivat potentiaalisesti aiheuttaa. Näitä tietoja analysoimalla voidaan määrittää pitääkö turvatoimenpiteitä lisätä tai kehittää. (Scarfone & Souppaya 2013, vi-vii.)

3.3 Hallintajärjestelmän tarvemäärittely

Yrityksen on suoritettava tarvemäärittely ja kartoitus siitä, minkälaisia ominaisuuksia he tarvitsevat omassa ympäristössään mobiililaitteiden tehokkaaseen hallintaan. Kun tarvemäärittely ja kartoitus on suoritettu, yritys hankkii yhden tai useamman hallintajärjestelmän, jotka tarjoavat määritellyt ominaisuudet. (Scarfone & Souppaya 2013, vii.) Hallintajärjestelmässä on hyvä olla ainakin seuraavat ominaisuudet.

Käyttöpolitiikan asettaminen

Hallintajärjestelmällä voidaan asettaa mobiililaitteisiin yrityksen tietoturvapolitiikan mukaiset käytännöt. Hallintajärjestelmän avulla voidaan myös kontrolloida tai rajoittaa mobiililaitteen käyttöjärjestelmää, applikaatioita ja teknisiä ominaisuuksia. Muita käyttöpolitiikan asettamiseen liittyviä ominaisuuksia ovat laitteen langattomien verkkorajapintojen hallinta, sekä asetetun politiikan seuranta ja raportointi, jos asetetusta käytännöstä poiketaan. (Scarfone & Souppaya 2013, vii.)

Tietoliikenne ja datan varastointi

Hallintajärjestelmällä on mahdollista tyhjentää kohdelaite kaikesta datasta ja käyttäjätiedoista etäyhteyden avulla. Ominaisuus on hyödyllinen esimerkiksi silloin, kun laite on varastettu tai vaarassa joutua tietovarkauden kohteeksi. (Scarfone & Souppaya 2013, vii.)

Käyttäjän ja laitteen tunnistus

Hallintajärjestelmän avulla voidaan pakottaa käyttäjä tunnistautumaan ennen kuin laitteella pääsee käsittelemään yrityksen tärkeitä resursseja. Muita yleisiä ominaisuuksia ovat

- mahdollisuus nollata mobiililaitteen salasana etähallinnan avulla
- mahdollisuus pakottaa PIN tai salasanakysely mobiililaitteeseen
- mahdollisuus lukita mobiililaite etähallinnan avulla (Scarfone & Souppaya 2013, vii).

Applikaatiot

Hallintajärjestelmä antaa mahdollisuuden rajoittaa mitä sovelluksia mobiililaitteeseen voidaan asentaa. Usein on myös mahdollista tehdä käyttöpolitiikka-asetus liittyen applikaatioiden asentamiseen. Käyttöpolitiikassa voidaan listata sekä sallitut että kielletyt applikaatiot. Muita yleisiä ominaisuuksia ovat

- mahdollisuus asentaa sekä päivittää applikaatioita mobiililaitteisiin etänä
- mahdollisuus rajoittaa mobiililaitteen käyttämiä synkronointipalveluja
- sovellusten ja applikaatioiden digitaalinen allekirjoittaminen ja verifiointi
- yrityksen omien applikaatioiden jakaminen hallintajärjestelmän mahdollistaman sovelluskirjaston avulla

- mahdollisuus estää tai rajoittaa pääsyä yrityksen resursseihin laitteilta, joissa on päivittämätön käyttöjärjestelmä tai vanha versio hallintajärjestelmän asiakasagentista (Scarfone & Souppaya 2013, vii).

3.4 Hallintajärjestelmän testaus ennen käyttöönottoa

Ennen kuin mobiililaitteiden keskitetty hallintajärjestelmä voidaan lopullisesti implementoida, on erittäin tärkeää suorittaa järjestelmän testausvaihe. Testausprosessissa pyritään arvioimaan järjestelmän toimintavarmuus, sopivuus yrityksen työympäristöön ja järjestelmän toimivuus eri laitteiden ja käyttöjärjestelmien kesken. Tärkeitä arvioitavia kohteita järjestelmän testauksessa ovat esimerkiksi yhteensopivuus, suojausominaisuudet, datan ja laitteiden varmentaminen, sovelluksen hallintaominaisuudet, ratkaisunhallinnan työkalut, lokikirjaus ja hallintajärjestelmän yleinen suorituskyky. (Scarfone & Souppaya 2013, vii.)

Ennen kuin hallintajärjestelmä implementoidaan virallisesti, on siihen tietoturvan kannalta suotavaa asentaa uusimmat päivitykset. Myös järjestelmän muut oheiskomponentit on syytä päivittää. Muita huomioon otettavia asioita on hallintajärjestelmän asetusten konfigurointi tietoturvallisten käytäntöjen mukaisesti. Rootattujen tai jailbreak-laitteiden automaattinen tunnistus on suotavaa ottaa käyttöön. (Scarfone & Souppaya 2013, vii.)

On myös tärkeää varmistaa, että hallintajärjestelmä ei automaattisesti palauta järjestelmän oletusasetuksia kohdatessaan kriittisen virheen (Scarfone & Souppaya 2013, vii).

3.5 Mobiililaitteiden suojaus ennen käyttöönottoa

Yrityksen mobiililaitteille on syytä tehdä perustason suojaus tietoturvauhkia vastaan ennen kuin laitteet luovutetaan loppukäyttäjille. Käytännössä tämä tarkoittaa, että mobiililaitteisiin määritellään yhtenäiset asetukset, jotka vastaavat yrityksen suunniteltua tietoturvapolitiikkaa.

Ennen mobiililaitteen käyttöönottoa on suotavaa, että suojattavan laitteen päivitykset ovat ajan tasalla, ja varmistettava, että hallintajärjestelmän käyttäjäagentti on asennettu mobiililaitteeseen. Tapauksissa, joissa mobiililaite on jo käyttöönotettu, mutta laitteessa käytetään tietoturvapolitiikan vastaisia asetuksia, on laitteeseen suositeltavaa palauttaa etäyhteyden avulla ylläpidon määrittämät tietoturvalliset asetukset. Perustason suojausta voidaan tukea asentamalla mobiililaitteisiin esimerkiksi virustorjuntaohjelmisto. (Scarfone & Souppaya 2013, vii.)

Laitehallinnassa tietoturvallinen käytäntö on palauttaa mobiililaite tehdasasetuksille tai vaihtoehtoisesti nollata laite hallintajärjestelmän avulla aina, kun laite luovutetaan uudelle käyttäjälle. Nollauksessa laite tyhjennetään applikaatioista, henkilökohtaisesta datasta, käyttäjäprofiileista sekä muusta tietoturvahyökkäyksille alttiista tiedosta.

3.6 Tietoturvapolitiikan säännöllinen ylläpito

Hyvään ylläpitoon lukeutuu uusimpien päivitys- ja korjaustiedostojen tarkistaminen ja asentaminen. Päivitysten toimintavarmuus on suositeltavaa testata ennen implementointia. Ylläpidon kehittämiseksi on tärkeää, että hallintajärjestelmä havaitsee ja kirjaa poikkeavuudet toimintaympäristössä. Lokiin kirjattava poikkeus voi esimerkiksi olla mobiililaitteen asetuksissa tapahtunut yrityksen asetetun tietoturvapolitiikan vastainen muutos. (Scarfone & Souppaya 2013, viii.)

Laitehallinnan helpottamiseksi on suositeltavaa pitää ajan tasalla olevaa inventaariota laitekannasta, laitteiden käyttäjistä, sekä laitteisiin asennetuista applikaatioista. Näillä toimenpiteillä pystytään esimerkiksi havaitsemaan laitteeseen asennettu applikaatio, joka on myöhemmin havaittu tietoturvariskiksi. Tällaisissa tapauksissa on harkittava, täytyykö laitteen pääsy yrityksen resursseihin evätä, tai poistaa applikaatio laitteesta etähallinnan avulla. (Scarfone & Souppaya 2013, viii.)

Lisäksi seuraavat menettelytavat lukeutuvat toimivaan ylläpitoon:

- On varmistettava, että hallintajärjestelmän jokainen komponentti on synkronoitu yhteiseen luotettavaan aikapalvelimeen.
- On tarkistettava järjestelmien ja resurssien käyttöoikeudet, sekä päivitettävä ne tarvittaessa.
- On suoritettava säännöllisesti arviointeja joissa selvitetään, noudatetaanko kohdelaitteissa yrityksen mobiililaitepolitiikkaa (Scarfone & Souppaya 2013, viii).

3.7 BYOD-politiikka

BYOD-termi muodostuu sanoista Bring Your Own Device. Käytännössä BYOD-politiikka on strategia, jossa työntekijät käyttävät omissa työtehtävissään itse valitsemiaan ja ostamiaan henkilökohtaisia laitteita. Tyypillisesti BYOD-politiikkaa sovelletaan älypuhelimien ja tablettien kanssa, käytäntöön voidaan myös sisällyttää perinteiset tietokoneet. Käytäntö tarkoittaa myös sitä, että työntekijät pääsevät omilla laitteillaan hyödyntämään yrityksen resursseja myös virallisen työajan ulkopuolella. (Alleau & Desemery 2013, 5.)

BYOD-politiikka on yleistynyt yhä enemmän siitä lähtien, kun älykkäät mobiililaitteet tulivat markkinoille. Politiikka asettaa kuitenkin sekä haasteita että hyötyjä yrityksille sekä näiden laitehallinnalle.

BYOD-politiikan hyödyt

Työnantajan näkökulmasta BYOD-politiikka voi tarjota seuraavia hyötyjä.

- **Pienemmät kustannukset**. Uusia mobiililaitteita tulee markkinoille nopeassa tahdissa, jolloin niiden hankkiminen ja päivittäminen voi tulla kalliiksi yritykselle. Yritys säästää kuluissa, koska BYOD-politiikassa työntekijä ostaa itse oman laitteensa. Näin työntekijä voi päivittää uusimpaan laitteeseen niin usein kuin haluaa ilman, että yritys joutuu maksajan rooliin (Gilmore & Beardmore 2013, 7). Työntekijät myös yleensä pitävät itse omistamistaan laitteistaan parempaa huolta (Chignell 2013).

- **Työntekijöiden tuottavuus kasvaa**. Tuottavuus voi kasvaa silloin, kun työntekijät pystyvät käyttämään omia mobiililaitteita työtehtävissään. Työntekijät voivat olla merkki- tai malliuskollisia tai heillä voi olla enemmän käyttökokemusta tietynlaisesta laitteesta, jolloin tämä voi auttaa työtehtävissä suoriutumista. (Gilmore & Beardmore 2013, 7.)
- **Työntekijöiden tyytyväisyys**. Työntekijät arvostavat mahdollisuutta valita mieluisa mobiililaite. Tämä puolestaan edistää työntekijöiden tyytyväisyyttä itse yritykseen ja sen toimitapoihin (Alleau & Desemery 2013, 5).

Työntekijöille BYOD-politiikka voi tarjoa seuraavia etuja:

- **Henkilökohtaisen laitteen suojaus**. Yritykset haluavat toteuttaa hyvää tietoturvapolitiikkaa, johon kuuluu laitteiden ja tärkeiden resurssien suojaaminen. Hyvää tietoturvapolitiikkaa voidaan toteuttaa esimerkiksi keskitetyllä virustorjuntaohjelmistolla. Tämän seikan ansiosta työntekijä voi saada omaan BYOD-politiikan mukaiseen mobiililaitteeseensa suojauksen täysin ilmaiseksi, sillä yleensä yritys hoitaa järjestelmien ylläpitoon ja lisensointiin liittyvät kulut. (Gilmore & Beardmore 2013, 8.)
- **Mielekkäämpi työympäristö**. Työntekijöiden tyytyväisyys yritykseen, työmotivaatio ja työn tuottavuus voivat kasvaa silloin, kun työntekijälle annetaan mahdollisuus suorittaa omia työtehtäviään omalla mieleisellä mobiililaitteella. (Gilmore & Beardmore 2013, 8.)

BYOD-politiikan haittapuolet

BYOD-politiikassa yrityksellä on yleensä rajallisesti vaikutusvaltaa siihen, minkälaisen mobiililaitteen työntekijät hankkivat itselleen. Yritys voi kuitenkin määritellä tietyt yleiset spesifikaatiot, jotka mobiililaitteesta täytyy löytyä. Yritykselle laitteen hankkimisessa huomionarvoisia seikkoja ovat esimerkiksi hankitun mobiililaitteen merkki, malli, käyttöjärjestelmä sekä yhteensopivuus yrityksen muiden laitteiden ja järjestelmien kanssa.

Laaja laitekanta voi kuitenkin vaikeuttaa keskitettyä mobiililaitteiden hallintaa. Laaja laitevalikoima voi laitehallinnan osalta kasvattaa IT-osaston työtehtävien määrää sekä kasvattaa laitteiden hallinnasta aiheutuvia kuluja. (Gilmore & Beardmore 2013, 9.)

BYOD-politiikka voi myös olla työntekijälle haittatekijä, jos yrityksellä ei ole tarjota perinteistä laitteen hankintastrategiaa. Perinteisessä mallissa yritys usein hoitaa laitteen hankinnan työntekijälle. Perinteisessä mallissa yritys myös yleensä vastaa laitteen huoltosuunnitelmasta, elinkaaresta sekä kustannuksista. (Drayton 2013.)

Jos BYOD-politiikka on yrityksen ainoa laitestrategia, on vaarana, että kaikki työntekijät eivät omista yrityksen tarpeiden mukaista laitetta tai eivät edes halua hankkia sellaista. BYOD-strategiassa huomioitavaa on myös huomioitava kuka hoitaa mahdolliset laitteen huolto tai -korjauskulut. (Drayton 2013.)

BYOD-politiikalla hankittuja mobiililaitteita käytetään usein myös työtehtävien lisäksi vapaa-ajalla. Tämä saattaa asettaa laitteet riskialttiimmaksi tietoturvahyökkäyksille ja haittaohjelmille. Saastumisen voi aiheuttaa esimerkiksi laitteeseen vapaa-ajalla ladattu applikaatio tai sähköpostin liitetiedosto. Saastuneet laitteet voivat aiheuttaa merkittäviä ongelmia esimerkiksi yrityksen sisäverkossa levittämällä haittaohjelmia yrityksen muihin laitteisiin. (Gilmore & Beardmore 2013.)

4 MOBIILILAITTEISIIN KOHDISTUVAT UHAT

4.1 Mobiililaitteisiin kohdistuvat fyysiset uhat

Mobiililaitteita käytetään tyypillisesti myös yrityksen ulkopuolisessa ympäristössä, jolloin mobiililaitteiden hallinnasta vastaavalla organisaatiolla ei aina ole suoraa fyysistä keinoa hallita puhelinta. Liikkuvuuden takia mobiililaitteet ovat alttiimpia varkauksille ja laitteiden katoamisille. (Juniper Networks 2011, 4.)

Suunniteltaessa mobiililaitteiden tietoturva- ja hallintapolitiikkaa, yritysten tulisi huomioida, että mobiililaitteet voivat joutua haitallisten osapuolten haltuun. Haitalliset osapuolet saattavat yrittää tunkeutua yrityksen arkaluontoisiin resursseihin, joko hyödyntämällä mobiililaitteiden haavoittuvuuksia suoraan tai välillisesti. (Scarfone & Souppaya 2013, 3-4.)

Fyysisten uhkien riskien minimointi

Fyysisten uhkien torjuntastrategia on syytä suunnitella kerroksittain.

Ensimmäinen kerros. Ensimmäisessä kerroksessa mobiililaitteelta vaaditaan pakollinen todentaminen ennen kuin laitteella pääsee käsiksi yrityksen resursseihin. Mobiililaitteella on usein oletusarvoisesti vain yksi käyttäjä, eikä siis erillistä tiliä jokaiselle mahdolliselle laitteen käyttäjälle. Näin ollen laitteeseen tarvitsee syöttää vain salasana todentamisen varmistamiseksi, eikä kokonaista käyttäjätunnusta. (Scarfone & Souppaya 2013, 4.)

Yksittäisen mobiililaitteen suojaamiseen käytetään yleensä PIN-koodia tai erillistä salasanaa, joka sisältää kirjaimia tai muita merkkejä. Salasanaa tai PIN-koodia kysytään esimerkiksi silloin, kun halutaan avata mobiililaitteen näytön lukitusruutu. Uusissa älypuhelimissa ja tableteissa todentamiseen voidaan käyttää esimerkiksi määrätyn kuvion piirtämistä, kasvojentunnistusta tai jopa sormenjälkitunnistusta. Nämä todennuskeinot ovat kaikissa nykyaikaisissa mobiilikäyttöjärjestelmissä sisäänrakennettuna.

Toinen kerros. Fyysisten uhkien torjuntastrategian toinen kerros keskittyy arkaluontoisen datan suojaamiseen. Suojaaminen voidaan toteuttaa salaamalla mobiililaitteen massamuisti sekä muistikortti. Toinen keino on linjata tietoturvapolitiikassa, että mobiililaitteessa on kiellettyä säilyttää arkaluontoista dataa. (Scarfone & Souppaya 2013, 4.)

Käytännön esimerkki fyysisestä uhasta on tilanne, jossa haitallinen taho voi junassa yrittää tarkkailla yrityksen työntekijän mobiililaitetta PIN-koodin tai salasanan toivossa.

Kolmas kerros. Kolmas ja viimeinen kerros keskittyy työntekijöiden kouluttamiseen ja yleiseen tietoturvan tiedottamiseen. Yrityksen tietoturvaa voidaan parantaa kouluttamalla työntekijöitä laitteiden oikeaoppiseen käyttöön. Organisaatio voi myös tiedottaa mahdollisista ajankohtaisista haavoittuvuuksista laitteissa, applikaatioissa, tietoliikenneyhteyksissä tai käyttöympäristöissä. (Scarfone & Souppaya 2013, 4.)

Käyttäjä on usein tietoturvan heikoin lenkki, joten koulutuksella voidaan merkittävästi vähentää käyttäjästä johtuvia tietoturvariskejä.

4.2 Varmistamattomat mobiililaitteet

Useista mobiililaitteista puuttuu tiettyjä tietoturvan kannalta tärkeitä ominaisuuksia. Mobiililaitteissa ei esimerkiksi käytetä TPM-turvapiiriä, joka on yhä useammin sisäänrakennettu esimerkiksi kannettaviin tietokoneisiin. (Scarfone & Souppaya 2013, 4.) TPM-turvapiiri on mikropiiri, jonka avulla tietokone tai järjestelmä voi käyttää yhä kehittyneempiä suojausominaisuuksia (Bond & Landrock 2011).

Yrityksen näkökulmasta BYOD-politiikan mukainen mobiililaite voi olla suurempi tietoturvariski kuin yrityksen omistama laite. Työntekijät ovat myös voineet jailbreikata tai rootata oman laitteensa. Jailbreikattu tai rootattu laite sallii allekirjoittamattomien applikaatioiden ajon, sisäänrakennettujen rajoitusten ohittamisen sekä käyttöjärjestelmän modifioinnin. Tietoturvapolitiikan kannalta on syytä huomioida, että mobiililaite, joka on käyttäjän toimesta jailbreakattu tai rootattu,

saattaa olla kasvanut riski yrityksen tietoturvalle (Scarfone & Souppaya 2013, 4.)

Jos laitteita ei pystytä hallitsemaan esimerkiksi roottauksen tai jailbreikkauksen mahdollistamien muokkausten takia, ovat ne lähtökohtaisesti yrityksen tietoturvan näkökulmasta epäluotettavia.

Varmistamattomien mobiililaitteiden riskien minimointi

Yrityksen on hyvä suunnitella toimintapolitiikka varmistamattomia laitteita varten.

Yksi vaihtoehto on rajoittaa BYOD-politiikan mukaisten laitteiden käyttöä yrityksessä, jolloin laitepolitiikassa suositaan ensisijaisesti yrityksen omistamia mobiililaitteita (Scarfone & Souppaya 2013, 4).

BYOD-politiikan mukaisten laitteiden tietoturvauhkaa voidaan minimoida sijoittamalla yrityksen tärkeät dataresurssit turvalliseen, muista resursseista erillään olevaan ympäristöön eli ns. Sandboxiin (Scarfone & Souppaya 2013, 4). Vaihtoehtoisesti BYOD-laitteet tai niissä ajettavat applikaatiot voidaan hallintajärjestelmän avulla sijoittaa toimimaan erillisessä turvallisessa Sandboxissa.

Mobiililaitteissa voidaan myös suorittaa haittaohjelmien skannauksia tietoturvan varmistamiseksi (Scarfone & Souppaya 2013, 4).

4.3 Varmistamattomat tietoliikenneyhteydet

Mobiililaitteet käyttävät lähes yksinomaan langattomia tietoliikenneyhteyksiä muodostaessaan verkkoyhteyden. Langattomia verkkoyhteyksiä voidaan muodostaa käyttämällä esimerkiksi Wi-Fi -yhteyksiä sekä datayhteyden mahdollistavia matkapuhelinverkkoja, esimerkiksi 3G-verkot.

Avoimet ja heikosti suojatut langattomat verkot asettavat haasteen laitteen hallinnalle ja valvonnalle. Avoimet ja suojaamattomat yhteystavat ovat alttiita sala-

kuuntelulla, mikä asettaa arkaluontoisen datan lähettämisen tai vastaanottamisen tietoturvan kannalta riskialttiiksi. Avoimet verkot voivat myös olla alttiita Man-in-the-middle -hyökkäyksille, joiden avulla haitallinen kolmas osapuoli voi siepata ja muokata viestiliikennettä. (Juniper Networks 2011, 4.)

Ellei ole ehdottoman varmaa, että mobiililaitetta käytetään vain ja ainoastaan yrityksen hallinnoimissa turvallisissa langattomissa verkoissa, on tietoturvapolitiikassa syytä olettaa, että mobiililaitteen ja valvomattomien verkkojen välinen yhteys on tietoturvariski (Scarfone & Souppaya 2013, 4).

Varmistamattomien tietoliikenneyhteyksien riskien minimointi

Varmistamattomien verkkojen riskejä voidaan minimoida seuraavin keinoin:

- Suosimalla vahvan salauksen ja todentamisen omaavia verkkotekniikoita, esimerkiksi VPN-verkkoyhteyttä.
- Rajoittaa tai estää turvattomien Wi-Fi -verkkojen käyttö. Erityisesti silloin, jos niissä käytetään haavoittuvaksi todettuja verkkoprotokollia.
- Myös kaikki mobiililaitteen käyttämättömänä olevat verkkorajapinnat voidaan kytkeä pois päältä. Esimerkiksi Wi-Fi -rajapinta voidaan kytkeä pois, kun käytetään 3G-mobiiliverkkoa. (Scarfone & Souppaya 2013, 5.)

4.4 Varmistamattomat applikaatiot

Applikaatioiden etsiminen, asentaminen ja käyttö on suunniteltu helppokäyttöiseksi älykkäissä mobiililaitteissa. Applikaatioita voidaan ladata mobiililaitteisiin myös kolmansien osapuolten sovelluskaupoista, mutta tämä voi aiheuttaa tiettyjä riskejä yrityksen tietoturvapolitiikalle. Kohonnutta tietoturvariskiä aiheuttavat laitteet, joihin on ladattu applikaatioita kolmannen osapuolen varmistamattomasta sovelluskaupasta. Käytännössä tämä tarkoittaa sitä, että varmistamattomissa sovelluskaupoissa ei välttämättä suoriteta perusteellista applikaatioiden testausprosessia ennen niiden julkaisua.

Yrityksen tietoturvapolitiikassa olisi syytä olettaa, että kolmansien osapuolien sovelluskaupoista ladattavat applikaatiot eivät ole oletusarvoisesti tietoturvallisia (Scarfone & Souppaya 2013, 5).

Varmistamattomien applikaatioiden riskien minimointi

Käyttöpolitiikassa voidaan kieltää tai estää kaikkien kolmansien osapuolien applikaatioiden asentaminen mobiililaitteeseen. Käyttöpolitiikassa voidaan myös ottaa käyttöön vain hyväksyttyjen applikaatioiden tarkistuslista, eli niin sanottu Application Whitelisting. (Scarfone & Souppaya 2013, 5.) Whitelisting-menetelmä toimii sillä periaatteella, että vain listalla olevat ylläpidon tarkistamat ja hyväksymät applikaatiot ovat asennettavissa käyttäjän mobiililaitteeseen.

Muita menetelmiä riskien minimointiin on tarkistaa, että asennetut applikaatiot saavat vain tarvittavat käyttöoikeudet mobiililaitteessa (Scarfone & Souppaya 2013, 5). Vaihtoehtoisesti voidaan sallia vain sellaisten applikaatioiden asentaminen, joissa applikaation vaatimat käyttöoikeudet eivät lähtökohtaisesti vaaranna tietoturvaa.

Mobiililaitteissa voidaan myös käyttää turvattua erillistä Sandbox-ympäristöä. Sandboxin avulla yrityksen tärkeät applikaatiot ja data voidaan eristää kaikesta muusta mobiililaitteen toissijaisesta datasta ja applikaatioista (Scarfone & Souppaya 2013, 5).

Vaikka varmistamattomien applikaatioiden riskien minimointi otettaisiin käyttöön, on tärkeää huomioida, että mobiililaitteet voivat silti päästä käsiksi varmistamattomaan Web-pohjaiseen sisältöön laitteen sisäänrakennetulla nettiselaimella (Scarfone & Souppaya 2013, 5).

Varmistamattoman Web-pohjaisen sisällön riskejä voidaan vähentää seuraavilla menetelmillä:

- pakottamalla mobiililaite käyttämään turvallisia yhdyskäytäviä, esimerkiksi VPN-yhteyksiä

- käyttämällä suojattuja HTTP-välityspalvelimia
- käyttämällä muita teknisiä keinoja, joissa URL-osoitteet ja muu Web-sisältö voidaan esikatsella tai arvioida ennen linkkien avaamista
- asentamalla mobiililaitteeseen erillinen selain, jota käytetään yksinomaan selaamaan yrityksen tärkeitä selainpohjaisia resursseja. Mobiililaitteen sisäänrakennettua nettiselainta voidaan käyttää selaamaan muuta ei-kriittistä sisältöä. (Scarfone & Souppaya 2013, 5.)

4.5 Vuorovaikutus muiden järjestelmien kanssa

Mobiililaitteet ovat vuorovaikutuksessa muiden järjestelmien kanssa vaihtaakseen tai tallentaakseen dataa, esimerkiksi datan synkronointi kahden laitteen välillä. Paikallinen vuorovaikutus järjestelmien välillä tapahtuu joko langallisesti kaapelin avulla tai vaihtoehtoisesti langattoman yhteyden avulla. (Scarfone & Souppaya 2013, 5.)

Vuorovaikutuksella voidaan myös esimerkiksi tarkoittaa langattoman verkkoyhteyden jakamista laitteiden kesken, tästä prosessista käytetään termiä tethering (Scarfone & Souppaya 2013, 5). Järjestelmien välinen vuorovaikutus voi myös tapahtua etäyhteyden avulla, esimerkiksi mobiililaite voi ottaa varmuuskopioita tiedostoista ja lähettää ne automaattisesti pilvipohjaiseen tallennusjärjestelmään.

Yrityksen tietoturvan kannalta riski on pienin silloin, kun yritys pystyy valvomaan kaikkia toisiinsa vuorovaikuttavia järjestelmiä ja laitteita. Käytännössä tämä on kuitenkin haastavaa toteuttaa, koska yksi tai useampi näistä komponenteista tai järjestelmistä on usein kolmannen osapuolen hallinnassa. Käytännön esimerkki tällaisesta tilanteesta on esimerkiksi yrityksen omistaman mobiililaitteen datan varmuuskopiointi kolmannen osapuolen pilvipohjaiseen tallennusjärjestelmään.

Järjestelmien vuorovaikutuksessa yhtenä merkittävänä tietoturvariskinä voidaan pitää yrityksen datan tai resurssien tallentamista varmistamattomaan kolmannen osapuolen palveluun tai järjestelmään. Tietoturvan kannalta on huomioita-

va, että järjestelmien välisessä vuorovaikutuksessa mahdolliset haittaohjelmat saattavat levitä laitteesta toiseen herkemmin. (Scarfone & Souppaya 2013, 5.)

Riskien minimointi järjestelmien vuorovaikutuksessa

Vuorovaikutuksen aiheuttamia riskejä voidaan lieventää rajoittamalla vuorovaikuttavia järjestelmiä, laitteita ja palveluita.

Jos yritys haluaa rajoittaa BYOD-mobiililaitteen kytkemistä tai synkronointia yrityksen omistamaan tietokoneeseen, täytyy tekniset tai ohjelmalliset rajoitukset toteuttaa tietokoneeseen. Jos taas yritys haluaa rajoittaa omistamansa mobiililaitteen kytkemistä tai synkronointia työntekijän BYOD-tietokoneeseen, on tekniset tai ohjelmalliset rajoitukset tehtävä yrityksen mobiililaitteeseen. (Scarfone & Souppaya 2013, 6.)

Datan varmuuskopiointia kolmannen osapuolen pilvipalveluihin voidaan rajoittaa teknisesti tai ohjelmallisesti. Mobiililaitteet ja niiden applikaatiot voidaan pyrkiä konfiguroimaan asetuksiltaan sellaiseksi, että laitteet eivät käytä datan tallennuksen yhteydessä kolmannen osapuolen pilvipalveluita (Scarfone & Souppaya 2013, 6).

4.6 Varmistamattoman sisällön käyttö

Mobiililaitteilla voi myös käyttää sisältöä, jota ei yleensä käytetä muissa tietoteknisissä laitteissa. Yleinen esimerkki tällaisesta sisällöstä on Quick Response Codet, eli QR-koodit, jotka on suunniteltu avattavaksi mobiililaitteen kameralla. QR-koodi on käytännössä viivakoodi ja jokainen QR-viivakoodi kääntyy tekstiksi tai merkkijonoksi. QR-koodi voi sisältää esimerkiksi URL-osoitteen, joka ohjaa avattaessa kohdelaitteen nettiselaimen QR-koodissa asetetulle verkkosivulle.

QR-koodeja voidaan käyttää myös haitallisella tavalla. QR-koodiin voidaan esimerkiksi istuttaa osoite, joka avattaessa ohjaa sivustolle, joka levittää haittaohjelmia (Scarfone & Souppaya 2013, 6).

Riskien minimointi varmistamattoman sisällön käytössä

Varmistamattoman sisällön riskejä voidaan minimoida kouluttamalla yrityksen työntekijöitä mahdollisista uhista sekä kehottamalla käyttäjiä olla avaamatta varmistamatonta sisältöä työkäyttöön tarkoitetulla mobiililaitteella (Scarfone & Souppaya 2013, 6). Turvallinen QR-koodin lukija-applikaatio mahdollistaa esikatselun avattavasta QR-koodista, ennen kuin käyttäjä joko hyväksyy tai hylkää sen sisällön.

Jos yrityksen verkkoasetukset sallivat, on mobiililaitteissa syytä käyttää turvallisia yhdyskäytäviä, varmistettuja välityspalvelimia, sekä muita teknisiä ratkaisuja, joilla voidaan ainakin osittain varmistaa URL-osoitteet ennen niiden avaamista (Scarfone & Souppaya 2013, 6).

Tilanteissa, joissa vaaditaan erittäin korkeaa tietoturvaa, voidaan keskitetyn hallintajärjestelmän avulla esimerkiksi estää mobiililaitteiden kameran käyttö (Scarfone & Souppaya 2013, 6). QR-koodeja ei voida avata mobiililaitteella, jos kamera ei ole käytettävissä, tämä voi ehkäistä mahdollisten haitallisten linkkien leviämisen.

4.7 Sijaintipalveluiden käyttö

Kaikissa moderneissa älypuhelimissa ja tableteissa on oletusarvoisesti GPS-valmius, joka mahdollistaa paikannuspalvelujen hyödyntämisen. GPS:n avulla paikannuspalvelut voivat esimerkiksi tarjota yrityksen yhteystietoja tai muita palveluita, jotka ovat fyysisesti lähellä käyttäjän sen hetkistä sijaintia. (Scarfone & Souppaya 2013, 6.) Paikannuspalveluja hyödynnetään paljon esimerkiksi sosiaalisessa mediassa, navigoinnissa sekä selainpohjaisissa palveluissa.

Paikannuspalveluita aktiivisesti hyödyntävät käyttäjät saattavat kuitenkin olla suuremmassa riskissä joutua tietoturvahyökkäyksen kohteeksi. Paikannuspalveluja hyödyntävät applikaatiot ja muut sovellukset kertovat lähes reaaliajassa, missä käyttäjä ja mobiililaite liikkuvat. Haitallinen taho voi hyödyntää tätä tietoa

toteuttaessaan tietoturvahyökkäystä. Tästä syystä paikannuspalvelut voidaan määrittää yrityksen tietoturvan sekä henkilökohtaisen yksityisyydensuojan riskitekijäksi. (Scarfone & Souppaya 2013, 6.)

Sijaintipalveluiden riskien minimointi

Sijaintipalveluiden riskejä voidaan ensisijaisesti minimoida rajoittamalla tai kieltämällä sijaintipalvelujen käyttö määrätyissä applikaatioissa ja palveluissa (Scarfone & Souppaya 2013, 6). Rajoittaminen tai kieltäminen voidaan usein toteuttaa keskitetyllä hallintajärjestelmällä.

Toinen keino riskien minimointiin on kouluttaa työntekijöitä sijaintipalveluiden käytössä (Scarfone & Souppaya 2013, 6). Työntekijöitä voidaan neuvoa olla käyttämättä sijaintipalveluita silloin, kun käyttöympäristö on varmistamaton ja turvaton.

On kuitenkin huomioitava, että käyttäjän sijainti voidaan nykyään paikantaa myös ilman GPS-yhteyttä. Yhä useampi web-sivusto tai applikaatio pystyy määrittämään käyttäjän sijainnin mobiililaitteen verkkoyhteyden perusteella. (Scarfone & Souppaya 2013, 6.) Sijainnin määrittäminen voidaan tehdä esimerkiksi IP-osoitteen tai käytettävän Wi-Fi -verkon perusteella.

Yritykset voivat kuitenkin myös hyötyä sijaintipalveluiden käytöstä. Hallintajärjestelmän avulla voidaan usein esimerkiksi asettaa räätälöity tietoturvapolitiikkaa sen mukaan, onko mobiililaite tietyllä hetkellä yrityksen turvallisessa käyttöympäristössä vai turvattomassa ulkopuolisessa käyttöympäristössä. (Scarfone & Souppaya 2013, 6.)

5 KESKITETYN HALLINTAJÄRJESTELMÄN TESTAUSSUUNNITELMA

5.1 Testauksen alkuasetelma ja tavoitteet

Opinnäytetyön toimeksiantoyritys Teleste oli siirtymässä vanhasta mobiililaitteiden hallintajärjestelmästä uuteen järjestelmään. Uuden järjestelmän ominaisuudet, toimintavakaus ja yhteensopivuus eri mobiililaitteiden kanssa oli testattava ennen hallintajärjestelmän virallista implementointia.

Uuden testattavan hallintajärjestelmän toimittaja oli Symantec. Koska uusi järjestelmä oli eri ohjelmistovalmistajan kehittämä, se ei ollut suoraan verrannollinen vanhaan järjestelmään. Hallintajärjestelmien eroavuuksien vuoksi oli erityisen tärkeää suorittaa testausprosessi ennen uuden järjestelmän implementointia. Hallintajärjestelmä asennettiin Telesten palvelimelle valtuutetun Symantec-kumppanin toimesta. Testausprosessi aloitettiin heti hallintajärjestelmän asentamisen jälkeen.

Opinnäytetyön tarkoituksena oli hallintajärjestelmän ja järjestelmän ominaisuuksien testaus. Hallintajärjestelmän asentaminen Telesten palvelimille ja testauksen jälkeinen implementointi eivät kuuluneet testausprosessiin.

Testauksen tavoitteena oli tutkia, miten uuden keskitetyn hallintajärjestelmän tarjoamat hallintaominaisuudet toimivat erityyppisissä mobiililaitteissa ja niiden erilaisissa käyttöjärjestelmissä. Testauksen tarkoituksena oli myös tutkia hallintajärjestelmän käyttöliittymän tarjoamia työkaluja laitteiden hallintaan. Tärkein näkökulma testauksessa oli se, esiintyisikö hallintajärjestelmän toiminnassa tai ominaisuuksissa kriittisiä virheitä, jotka saattaisivat estää hallintajärjestelmän implementoinnin.

Testaustulokset on nähtävissä tämän opinnäytetyön liitteestä 1.

5.2 Symantec Mobile Management -hallintajärjestelmän kuvaus

Symantec Mobile Management eli lyhennettynä SMM, on skaalautuva hallintajärjestelmä, jonka avulla yritykset voivat turvata ja hallita omistamiaan mobiililaitteita.

Symantec tarjoaa useita versioita Mobile Management -järjestelmästään. Esimerkiksi Symantec Mobile Management Suite kokoaa kaikki mobiilihallintaan liittyvät ominaisuudet yhteen ohjelmistopakettiin (Kuva 2)

	Mobile Management	App Center	Symantec Mobile Management Suite Try it now
MDM with compliance and blacklisting	✓		✓
Unified management for laptops, macs, smartphones and tablets	✓		✓
Distribution of in-house, cloud or 3rd party apps	✓	✓	✓
App and data protection with mobile data leakage protection		✓	✓
App Authentication and Single Sign-On		✓	✓
BYOD, MDM and secure corporate email		✓	✓
Ecosystem of wrapped-apps, including third party apps		✓* (with Symantec Sealed Program)	✓
Mobile malware protection for Android and Windows Mobile			✓* (with Symantec Mobile Security)

Kuva 2. Symantec Mobile Management -ohjelmistopaketit (Symantec 2014).

Symantec Mobile Management on lisenssipohjainen järjestelmä, tarvittavat lisenssit hankitaan yrityksen hallittavien mobiililaitteiden kokonaismäärän mukaan. Testausprosessia varten ei tarvinnut hankkia lisää laitelisenssejä.

Järjestelmävaatimukset

Symantec Mobile Management voidaan asentaa joko erillisenä itsenäisenä järjestelmänä (standalone) tai jo valmiiksi asennetun Symantec ITMS -järjestelmän lisäosaksi. ITMS muodostuu sanoista IT Management Suite ja sen tarkoituksena on helpottaa yrityksen asiakaspäätteiden ja palvelimien hallintaa. ITMS:n avulla kaikki tarvittavat Symantec-hallintajärjestelmät yhdistetään yhden keskitetyn käyttöliittymän taakse. Symantec käyttää tästä hallinta-alustasta nimeä Symantec Management Platform. Management Platformin avulla yritys voi virtaviivaistaa ja tehostaa omia IT-palveluitaan sekä resurssejaan.

Symantec Mobile Management standalonen järjestelmävaatimukset ovat:

- Microsoft Windows 2008 Enterprise Edition
- Microsoft SQL Server 2005/2008.

Symantec Mobile Management ITMS -versio voidaan lisätä suoraan olemassa olevaan ITMS-infrastruktuuriin.

Tämän opinnäytetyön testausprosessi suoritettiin Symantec Mobile Management ITMS -versiolla.

Käyttäjäagentit

Hallintajärjestelmän käyttäjäagentti on mobiililaitteen applikaatio, jonka käyttäjät asentavat omaan laitteeseensa, yhdistääkseen ja rekisteröidäkseen kyseisen mobiililaitteen yrityksen keskitettyyn hallintajärjestelmään. Käyttäjäagentti on ladattavissa mobiililaitteisiin käyttöjärjestelmän omasta natiivista sovelluskaupasta. Esimerkiksi Android-käyttöjärjestelmälle agentin voi ladata virallisesta Google Play -sovelluskaupasta.

Testausympäristössä kaikki käyttäjäagentit ladattiin mobiililaitteisiin käyttöjärjestelmien natiiveista virallisista sovelluskaupoista. Järjestelmän virallisessa im-

plementoinnissa olisi hyvä kehittää ratkaisu, jolla käyttäjäagentti saataisiin automatisoidusti asennettua jokaiseen yrityksen hallittavaan mobiililaitteeseen.

Hallintajärjestelmän käyttäjäagentit on erikseen kehitetty jokaiselle mobiilikäyttöjärjestelmän rajapinnalle. Käyttäjäagentit pyrkivät tarjoamaan tasavertaiset hallintaominaisuudet jokaiselle käyttöjärjestelmälle. Testausprosessin aikana kävi kuitenkin ilmi, että osa mobiililaitteiden käyttäjäagenteista ei pystynyt tarjoamaan kaikkia mahdollisia hallintaominaisuuksia tasavertaisesti. Käyttäjäagenttiapplikaation käyttöliittymä on kuitenkin lähes identtinen eri mobiilikäyttöjärjestelmien välillä.

Käyttäjäagentti päivittää ja ilmoittaa kyseisen mobiililaitteen tilan säännöllisin väliajoin yrityksen mobiililaitteiden hallintajärjestelmälle, tästä käytetään englanninkielistä termiä polling. Käyttäjäagentti hakee reaaliajassa hallintajärjestelmän palvelimelta annetut komennot, tiedostot ja päivitykset. Käyttäjäagentti lähettää taas puolestaan tietoja mobiililaitteesta ja sen käyttäjästä keskitetylle hallintajärjestelmälle.

Tiivistetysti voidaan sanoa, että laitehallinnan käyttäjäagentin asentaminen mobiililaitteeseen tuo kattavan määrän lisää hallintaominaisuuksia. Jos tietylle mobiilikäyttöjärjestelmälle ei ole ladattavissa käyttäjäagenttia, voidaan laitehallintaa toteuttaa Microsoftin Exchange ActiveSyncin avulla. Valitettavasti Exchange ActiveSync ei tarjoa kaikkia samoja hallintaominaisuuksia kuin käyttäjäagentit.

Exchange ActiveSync tarjoaa kuitenkin paljon sellaisia ominaisuuksia, joihin pelkkä käyttäjäagentti ei pysty. Exchange ActiveSyncin avulla voidaan esimerkiksi lähettää politiikka-asetukset yhtäaikaisesti moneen eri mobiililaitteeseen. On kuitenkin tärkeää huomioida, että Exchange ActiveSyncin kautta asetetut politiikka-asetukset saattavat toimia eri tavoin riippuen siitä, mikä mobiilikäyttöjärjestelmä kohdelaitteessa on.

Mobiilihallinnan näkökulmasta parhaaseen tulokseen päästään silloin, kun kohdelaitteessa käytetään rinnakkain käyttäjäagentin sekä Exchange ActiveSyncin tarjoamia hallintaominaisuuksia.

Symantec Mobile Management tarjoaa laitehallinnan käyttäjäagentit seuraaville käyttöjärjestelmille:

- Apple iOS 4.1 ja sitä uudemmat versiot
- Google Android 2.2 ja sitä uudemmat versiot
- Microsoft Windows Phone 7 ja 7.5
- Microsoft Windows Mobile 6.1 ja 6.5
- Symbian v5.0.50.

SMM tarjoaa Googlen Android-käyttöjärjestelmälle natiivin agenttipohjaisen hallinnan lisäksi myös valinnaisena lisäosana sähköpostiasiakasohjelman.

Apple iOS -käyttöjärjestelmän mobiililaitteet käyttävät Applen Push Notification Serviceä keskitetyn hallintajärjestelmän ja hallittavan mobiililaitteen väliseen kommunikaatioon (käyttäjäagentti).

Google Android -käyttöjärjestelmään pohjautuvat mobiililaitteet käyttävät vastaavanlaiseen hallintajärjestelmän ja hallittavan mobiililaitteen väliseen kommunikaation Google Cloud Messaging (GCM) -palvelua (käyttäjäagentti).

Microsoft Exchange ActiveSync

Microsoft Exchange ActiveSync, josta käytetään lyhennettä EAS, on protokolla, joka on suunniteltu synkronoimaan dataa yrityksen viestinpalvelimen ja työntekijän mobiili- tai muun päätelaitteen välillä. EAS on suunniteltu synkronoimaan kaksisuuntaisesti esimerkiksi sähköpostin, yhteystiedot, kalenterin, tehtävät sekä muistiinpanot. Kuten jo aiemmin on mainittu, protokolla myös mahdollistaa mobiililaitteiden hallintaan liittyvien komentojen antamisen.

EAS on myös tärkeä komponentti Symantec Mobile Managementissa. SMM:ssä Exchange ActiveSync mahdollistaa mobiililaitteen hallinnan, rooli-pohjaisen käyttöpolitiikan asettamisen sekä yksittäisten laitteiden tai ryhmien tietojen katselun tai keräämisen hallintajärjestelmän käyttöliittymän avulla. EAS:n tarjoamat

hallintaominaisuudet riippuvat käytettävästä EAS:n versionumerosta, uudemmat EAS-versiot tarjoavat kaikkein kattavimmat hallintaominaisuudet.

5.3 Testausympäristö ja laitteet

Hallintajärjestelmän testaus suoritettiin Telesten tiloissa, hyödyntämällä yrityksen langattomia verkkoja sekä resursseja. Testaus suoritettiin pääosin yrityksen sisäverkossa, joten käyttötapaukset eivät täysin vastaa implementoinnin jälkeistä käyttöympäristöä. Käyttöympäristö vastasi kuitenkin riittävästi realistista käyttötilannetta, eikä testausta toteutettu esimerkiksi emuloimalla tai täysin virtuaalipohjaisesti toteutettuna.

Testauksen suunnittelussa, käyttötapauksien ja tulosten kirjaamisessa käytettiin apuvälineenä yrityksen tietokonetta. Testausprosessin tapahtumien kirjaamiseen käytettiin Microsoft Wordia, Notepadia sekä kuvakaappauksia ja videokuvaa hallintajärjestelmästä ja mobiililaitteiden käyttäjäagenttien käyttöliittymästä.

Kaikki testissä käytetyt mobiililaitteet olivat yrityksen omistamia resursseja. Testauksessa käytössä ollut SIM-kortti oli myös yrityksen omistama. Testaustapauksia tehtiin käyttämällä sekä datayhteyttä, että yrityksen Wi-FI -verkkoja.

Testausta tehtiin usealla eri valmistajan laitteella ja käyttöjärjestelmäalustalla (Taulukko 1). Testausta tehtiin sekä tableteilla että älypuhelimilla.

Taulukko 1. Testauksessa käytetyt mobiililaitteet.

Laitemalli	Laitetyyppi	Käyttöjärjestelmä	Huomioitavaa
Apple iPad 3rd. generation	Tabletti	Apple iOS 5.1.1	
Nokia Lumia 710	Älypuhelin	Microsoft Windows Phone 7.5	
Nokia Lumia 800	Älypuhelin	Microsoft Window Phone 7.5	
Nokia 700	Älypuhelin	Symbian Belle	Ei käyttäjäagenttia saatavilla.
Samsung Galaxy Tab2 10.1	Tabletti	Google Android 4.0.4	
ZTE Blade	Älypuhelin	Cyanogenmod	Rootattu laite. Cyanogenmod on epävirallinen Android jakelu.

Keskitetyn hallintajärjestelmän testausta suoritettiin seuraavilla järjestelmäversioilla:

- Symantec Mobile Management 7.2 MR1
- Symantec Mobile Management 7.2 SP1

Testaustyön alkuvaiheessa SMM:n versionumero oli 7.2 MR1. Testausprosessin myöhemmässä vaiheessa järjestelmästä julkaistiin uusi versio 7.2 SP1. Hallintajärjestelmän versionumero 7.2 SP1 toi joitain pieniä uudistuksia ja ominaisuuksia hallintajärjestelmään. Lisäksi päivityksessä korjattiin järjestelmässä esiintyneitä lapsentauteja. Hallintajärjestelmän päivitykset eivät vaikuttaneet mainittavasti itse testausprosessiin ja sen tuloksiin. Päivitys toi kuitenkin joitain uusia ominaisuuksia, joista testattiin applikaatioiden kieltolista eli Application Blacklisting.

Testauksen tarkoituksena oli selvittää, miten hallintajärjestelmän eri ominaisuudet toimivat eri laitteissa. Testauksessa kirjattiin muistiin suoritetut käyttötapa-

ukset ja miten käytetyt ominaisuudet toimivat kohdelaitteissa. Muistiin kirjattiin myös järjestelmän testauksessa havaitut haasteet ja ongelmat.

5.4 Testausmenetelmät

Testauksen alkuvaiheessa mobiilikäyttöjärjestelmille ja näiden ekosysteemeille luotiin omat käyttäjätunnukset testausprosessia varten. Nämä tunnukset luotiin ainoastaan testikäyttöä varten. Käyttäjätunnukset luotiin seuraaville käyttöjärjestelmille:

- Windows Phone Live-ID (Microsoft Windows Phone -käyttöjärjestelmä)
- Apple ID (Apple iOS -käyttöjärjestelmä)
- Google Account (Google Android -käyttöjärjestelmä).

Windows Live-ID on sähköpostiosoite ja salasana, joita käytetään kirjautuessa mm. seuraaviin Microsoftin ekosysteemin palveluihin:

- Messenger -pikaviestin
- Oman puhelimen paikantaminen
- OneDrive (entinen SkyDrive) -pilvipohjainen verkkotallennustila.

Apple ID on käyttäjätunnus Applen ekosysteemin palveluihin, kuten

- iTunes Storeen
- iCloudin käyttöönottoon
- Applen -tukisivustolle.

Google Account on käyttäjätunnus esimerkiksi seuraaviin Googlen ja Androidin palveluihin:

- Play Store -sovelluskauppaan
- Gmail -sähköpostipalveluun.

Näitä luotuja testitunnuksia käytettiin mobiililaitteiden käyttöönotossa, johon kuului esimerkiksi hallintajärjestelmän käyttäjäagentin lataaminen käyttöjärjestelmän virallisesta sovelluskaupasta.

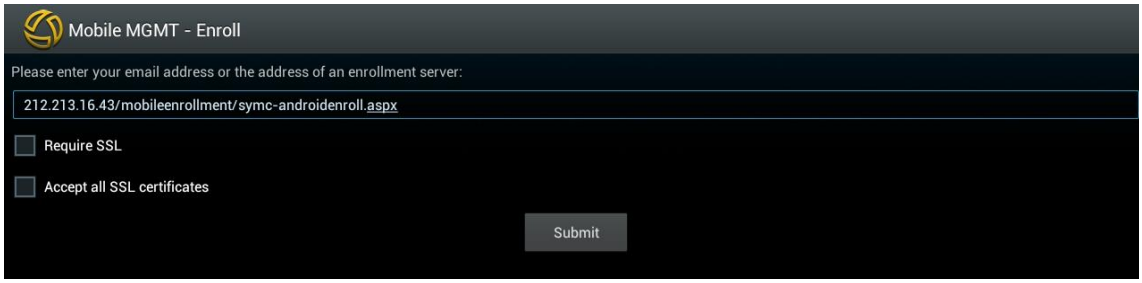
Keskitettyä hallintajärjestelmää varten luotiin tarvittavilla käyttöoikeuksilla varustettu Active Directory käyttäjätunnus ja salasana yrityksen domainiin. Active Directory (AD) on Microsoftin Windows-toimialueen käyttäjätietokanta ja hakemistopalvelu. Käyttäjätunnuksen nimeksi luotiin matti.mouho. Tämän testitunnuksen sähköpostiosoitteeksi muodostui matti.mouho@teleste.com

Käyttäjäagentti asennettiin kaikkiin niihin käyttöjärjestelmiin joihin se oli saatavilla. Käyttäjäagentti ladattiin käyttöjärjestelmän virallisesta sovelluskaupasta. Laitteisiin, johon käyttäjäagenttia ei ollut saatavilla, ei luonnollisesti voitu kohdistaa testitapauksia, joissa tutkittiin käyttäjäagentin ominaisuuksia ja toimivuutta.

Testauksessa jokaista ominaisuutta testattiin vähintään kaksi kertaa (2x), minkä jälkeen kirjattiin käyttötapauksen havainnot ja tämän jälkeen testattava mobiililaite tyhjennettiin kokonaan (wipe) joko hallintajärjestelmän avulla tai mobiililaitteen omista asetuksista. Laitteen tyhjentämisellä haluttiin välttää mahdollisten muiden laiteasetusten tai ominaisuuksien konfliktit tai muu vaikutus sillä hetkellä testattavaan ominaisuuteen.

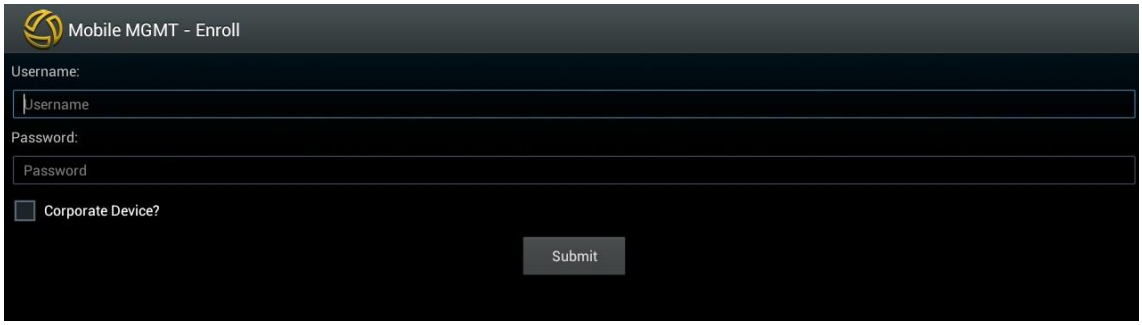
Testattavan mobiililaitteen oletustila ennen testaustapauksia (default state)

1. Tyhjennetään mobiililaite käyttäjätileistä ja applikaatioista ennen uuden käyttötapauksen testaamista.
2. Otetaan testattava mobiililaite käyttöön ja tehdään käyttöönotto hyödyntämällä ennalta luotuja käyttöjärjestelmän/ekosysteemin testitunnuksia (esim. Apple -käyttöjärjestelmän laitteissa Apple ID -käyttäjätunnuksia).
3. Ladataan mobiililaitteen käyttöjärjestelmän virallisesta sovelluskaupasta Symantec Mobile Management -käyttäjäagentti.
4. Avataan käyttäjäagentti ja syötetään tyhjään kenttään SMM -palvelimen osoite. Testausprosessissa kenttään syötettiin aina itse palvelimen osoite, eikä vaihtoehtoisesti testikäyttäjän sähköpostiosoitetta (Kuva 3).



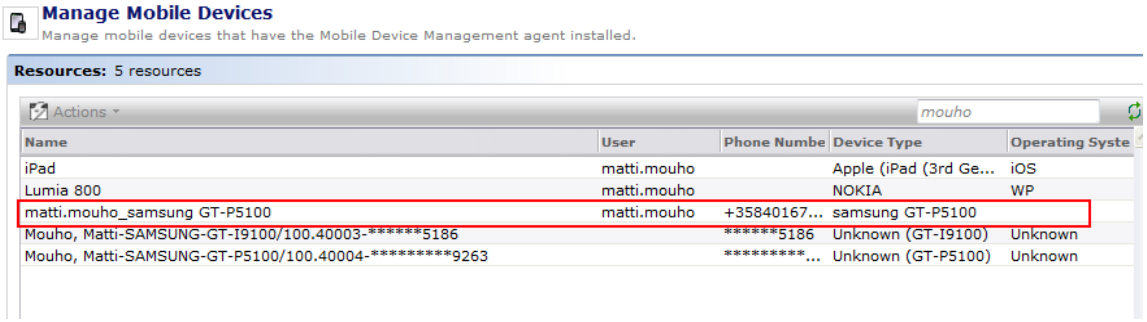
Kuva 3. Android-käyttäjäagentin yhdistäminen hallintapalvelimeen.

5. Jos yhdistäminen hallintapalvelimeen onnistuu -> syötetään käyttäjä-agentti applikaatioon omat AD-testikäyttäjätunnukset. Tässä tapauksessa testikäyttäjätunnus matti.mouho (Kuva 4).



Kuva 4. Käyttäjätietojen syöttäminen käyttäjäagenttiin.

6. Hyväksytään loppukäyttäjän lisenssisopimus (EULA) ja applikaation tarvitsemat laitteen käyttöoikeudet.
7. Tarkistetaan Symantec Mobile Management -hallintajärjestelmästä, että laite on hyväksynyt laitteen ja käyttäjän enrollmentin/rekisteröinnin (Kuva 5).



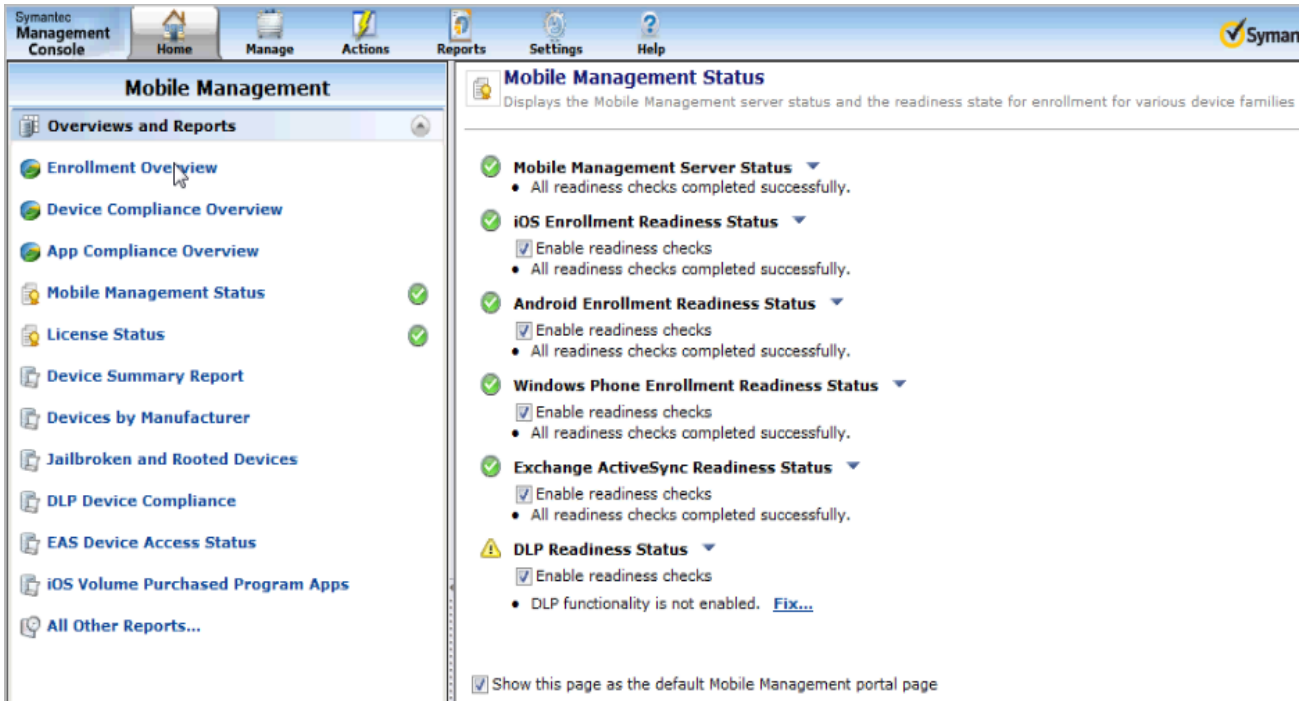
Kuva 5. Hyväksytty laitteen ja käyttäjän rekisteröinti hallintajärjestelmään.

8. Testataan haluttu ominaisuus tai käyttötapaus, minkä jälkeen kirjataan testauksen havainnot.
9. Palataan kohtaan 1. ja tyhjennetään mobiililaite (device wipe) kaikesta sisällöstä ja tämän jälkeen voidaan testata seuraavaa ominaisuutta.

Symantec Mobile Management -hallintajärjestelmän käyttöliittymä testaustapauksissa

1. SMM -hallintajärjestelmän käyttöliittymään kytkeydytään Web-selaimen avulla. Hallintajärjestelmän palvelimen nimi oli Borex. Borex -palvelimen osoite syötettiin selaimen osoitekenttään
2. SMM -hallintajärjestelmän käyttöliittymä toimi oikeaoppisesti vain Internet Explorer -selaimella. Käyttöliittymää kokeiltiin esimerkiksi Mozilla Firefox -selaimella, mutta käyttöliittymä ei toimi silloin oikeaoppisesti
3. SMM -hallintajärjestelmän käyttöliittymän päänäkymä on esitetty kuvassa 6. Päänäkymästä pystyy nopeasti navigoimaan haluttuun järjestelmän osa-alueeseen.

4. Lähes kaikki testattavat ominaisuudet annettiin suoraan hallintajärjestelmän käyttöliittymän kautta.

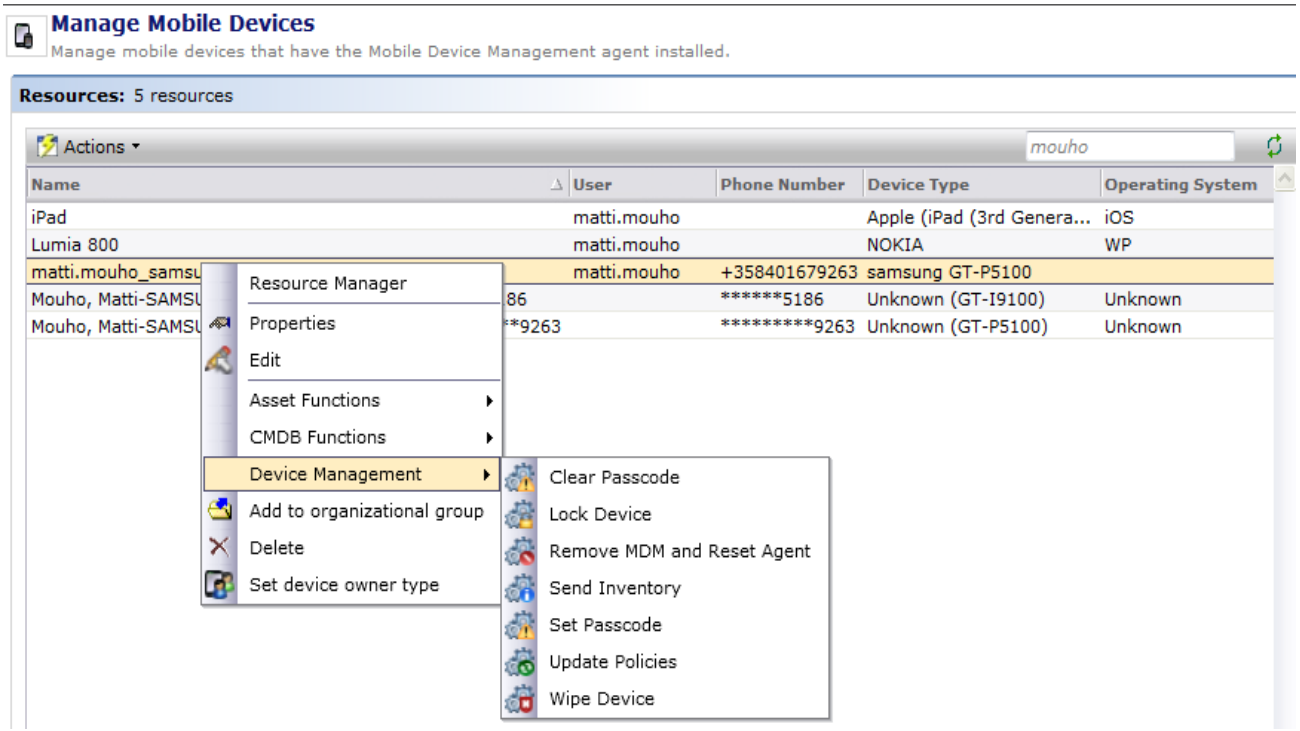


Kuva 6. Symantec Mobile Console / Mobile Management -etusivunäkymä.

6 HALLINTAJÄRJESTELMÄN TESTATUT OMINAISUUDET

Symantec Mobile Management -hallintajärjestelmä on massiivinen kokonaisuus, joka sisältää satoja hallintaan liittyviä ominaisuuksia ja komponentteja. Koska testausprojektilla oli vain rajalliset aikaresurssit ja testaajia vain yksi henkilö, ei kaikkia ominaisuuksia pystytty testaamaan. Testaustulokset ja testaukseen liittyvät huomiot löytyvät tämän opinnäytetyön liitteestä 1.

Testauksen pääpaino haluttiin asettaa tärkeimpiin laitehallinnan ominaisuuksiin. Tässä luvussa on listattu tärkeimmät testatut ominaisuudet. Yhdeksi tärkeimmäksi ominaisuudeksi asetettiin Device Management -komennot. Näihin komentoihin kuuluvat mm. salasanan poistaminen kohdelaitteesta, laitteen etälukitus ja laitteen tyhjentäminen etänä (Kuva 7).



Kuva 7. Device Management -hallintaominaisuudet.

Salasanan poistaminen kohdelaitteesta (Clear Passcode)

Clear Passcode -komento poistaa kohdelaitteesta asetetun salasanan. Ominaisuus on hyödyllinen esimerkiksi silloin, kun työntekijä on unohtanut laitteensa salasanan.

Kohdelaitteen etälukitus (Lock Device)

SMM tarjoaa mahdollisuuden lukita haluttu mobiililaite etähallinnan avulla. Kun komento annetaan hallintajärjestelmästä, lukitsee se halutun kohdelaitteen.

Hallintajärjestelmän ja mobiililaitteen hallintayhteyden resetoiminen (Remove MDM and Reset Agent)

Kyseinen komento poistaa yhteyslinkin hallintajärjestelmän ja kohdelaitteen välillä. Kun komento on annettu, täytyy kohteena ollut mobiililaite rekisteröidä/yhdistää (enroll) uudelleen hallintajärjestelmään.

Kohdelaitteen tietojen päivitys hallintajärjestelmään (Send Inventory)

Send Inventory -komento lähettää kohteena olevan mobiililaitteen tiedot hallintajärjestelmälle.

Laitteen etätyhjennys hallintajärjestelmän avulla (Wipe Device)

SMM tarjoaa mahdollisuuden tyhjentää haluttu mobiililaite kaikesta sisällöstä etähallinnan avulla. Wipe Device -ominaisuus tyhjentää laitteesta käyttäjätilit ja applikaatiot.

Pääsykoodin pakottaminen kohdelaitteeseen (Set Passcode)

Sett Passcode -komennon avulla kohdelaitteeseen voidaan pakottaa pääsykoodi.

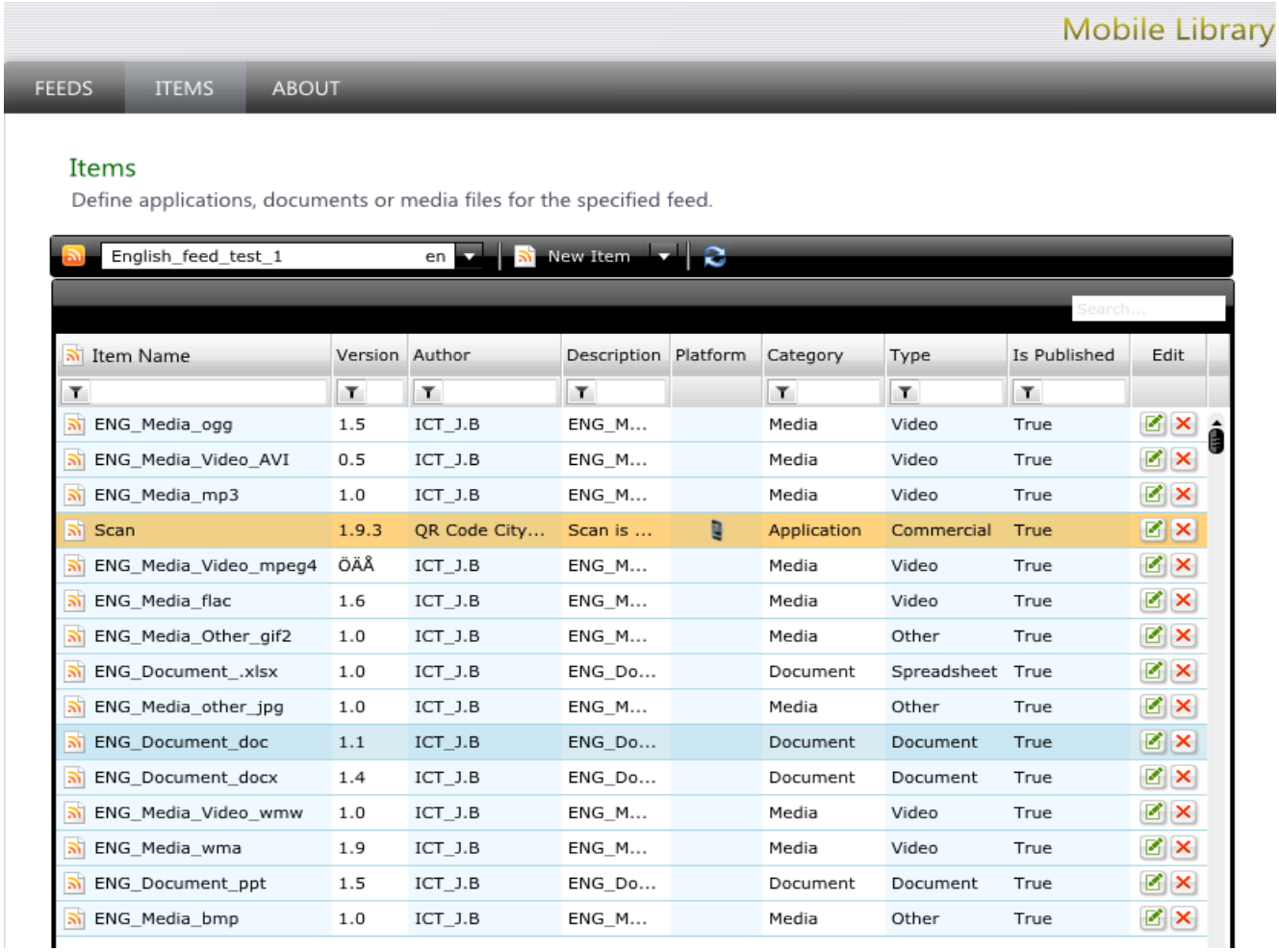
Mobiililaitteen rekisteröinti hallintajärjestelmään (Enroll)

Testaustapauksessa selvitettiin, onnistuiko kaikkien laitteiden rekisteröinti hallintajärjestelmään ilman ongelmia. Tämä testitapaus suoritettiin vain mobiililaitteille, joihin käyttäjäagentti oli saatavilla.

Hallintajärjestelmän sovelluskirjasto (Mobile Library)

Mobile Library on RSS-pohjainen sovelluskirjasto, johon voidaan lisätä esimerkiksi applikaatioita, yksittäisiä tiedostoja sekä tiedotteita RSS-syötteinä (Kuva 8). RSS-syöte on tapa, jolla sisällön julkaisijat voivat helposti levittää päivittyvää digitaalista sisältöä standardoidussa muodossa. Mobile Libraryyn lisätyt objektit näkyvät hallintajärjestelmään rekisteröityneen mobiililaitteen käyttäjäagentissa.

Tässä testitapauksessa haluttiin selvittää, toimiko objektien lisääminen hallintajärjestelmään ja miten ne toimivat mobiililaitteiden käyttäjäagenteissa. Testaustapaukseen kuului myös selvittää, miten eri tiedostotyypit toimivat tässä sovelluskirjastossa ja miten ne reagoivat mobiililaitteissa.



Kuva 8. Mobile Library -hallintajärjestelmän sisäinen sovelluskirjasto.

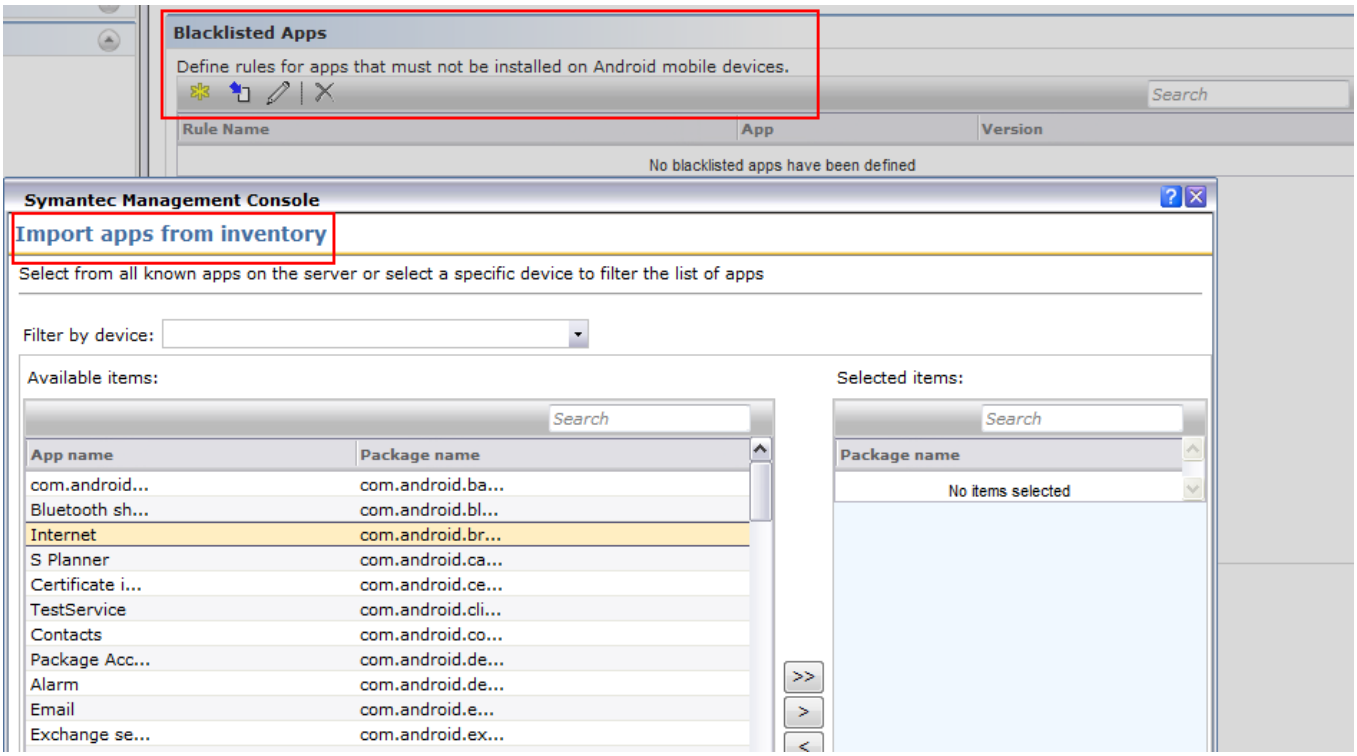
Jailbreak ja rootatut laitteet

Tässä testitapauksessa haluttiin selvittää, miten hallintajärjestelmä reagoi mobiililaitteen jailbreakiin tai roottaukseen.

Applikaatioiden kieltolista (Application Blacklisting)

Application Blacklisting -ominaisuuden avulla voidaan luoda lista applikaatioista jotka ovat yritysympäristössä kiellettyjä. Kieltolista voidaan tehdä joko määrittämällä kiellettävän applikaation spesifikaatiot tai valitsemalla hallintajärjestelmän valmiista applikaatiolistasta kiellettävä sovellus (Kuva 9). Kieltolista ei estä applikaatioiden käyttämistä tai asentamista, mutta hallintajärjestelmä tilastoi hallit-

tavista mobiililaitteista löytyvät kielletyt applikaatiot. Näiden tilastojen ja raporttien pohjalta yritys voi halutessaan suorittaa jatkotoimenpiteitä.



Kuva 9. Application Blacklisting -ominaisuus.

Exchange ActiveSync -ominaisuudet ja käyttöpolitiikka-asetukset (Policy)

Exchange ActiveSyncin kautta pystyy antamaan laitehallintaan liittyviä käskyjä, kuten kohdelaitteen tyhjentäminen etänä. Testauksessa seurattiin, miten nämä hallintaominaisuudet toimivat kohdelaitteissa.

Exchange ActiveSyncin avulla on mahdollista luoda käyttöpolitiikka, joka voidaan ajaa halutuille mobiililaitteille etänä. Politiikka voi sisältää pakottavia asetuksia esimerkiksi käyttäjän mobiililaitteen pääsykoodin pituudesta.

Hallintajärjestelmän raportointityökalut

Hallintajärjestelmän avulla voidaan luoda raportteja esim. laitemääristä ja käyttäjistä. Tässä testitapauksessa tutkittiin, onnistuuko raporttien luonti ja mitä dataa raportit kertovat.

7 YHTEENVETO JA JOHTOPÄÄTÖKSET

Tämän opinnäytetyön tarkoituksena oli suorittaa mobiililaitteiden hallintajärjestelmän testausprosessi. Testauksen tavoitteena oli selvittää uuden hallintajärjestelmän toimintavarmuus, ominaisuudet ja yhteensopivuus erilaisten mobiililaitteiden kanssa. Testauksen ehkä tärkein päämäärä oli testata, onko hallintajärjestelmästä tai sen hallintaominaisuuksista, jokin niin laaja ongelma tai haaste, joka voisi estää järjestelmän virallisen implementoinnin. Testaus tehtiin toimeksiantona Telestelle.

Opinnäytetyön teoriaosuudessa perehdyttiin mobiililaitteiden ominaispiirteisiin, käyttöjärjestelmiin, turvallisen laitehallinnan menetelmiin sekä mobiililaitteisiin kohdistuviin uhkiin. Teoriaosuus loi tietopohjan hallintajärjestelmän testaamiselle.

Hallintajärjestelmän testausta varten laadittiin suunnitelma. Testaussuunnitelmassa käsiteltiin testauksen alkuasetelma ja tavoitteet, hallintajärjestelmän kuvaus, testausympäristö ja laitteet sekä testausmenetelmät. Testaussuunnitelman lisäksi määritettiin hallintajärjestelmän testattavat ominaisuudet. Nämä asiat alustivat testaustyön ja testaustulokset.

Testaustulosten pohjalta voitiin selvittää, toimiko suurin osa hallintajärjestelmän perusominaisuuksista toivotulla tavalla. Testauksessa kohdattiin kuitenkin myös useita haasteita.

Testaustyötä vaikeutti hallintajärjestelmän sertifikaatteihin liittyneet ongelmat. Varsinkin testauksen alkuvaiheessa sertifikaattiongelmat jopa lykkäsivät tiettyjen laitteiden testausta. Toinen testaamisprosessia vaikeuttava asia oli testausympäristön langattomien verkkojen tiukat palomuurisäännöt. Tiukat asetukset aiheuttivat välillä tilanteita, joissa testattava mobiililaite ei pystynyt vastaanottamaan hallintajärjestelmän antamia hallintakomentoja. Tätä ongelmaa pystyttiin kuitenkin osittain kiertämään käyttämällä mobiililaitteen datayhteyttä tai muuta yrityksen langatonta verkkoyhteyttä. Testiympäristö ei vastannut täysin oikeata implementointiympäristöä, joten ainakin osa ongelmista korjaantuu jo

sillä, kun hallintajärjestelmä siirretään pois testiympäristöstä viralliseen käyttöön.

Pois lukien edellä mainitut ongelmat, ei testauksen aikana havaittu ylitsepääsemättömiä virheitä tai ongelmia. Tärkeimmät hallintaominaisuudet toimivat pääosin oikealla tavalla. Jos virheitä havaittiin, ne harvoin olivat ylitsepääsemättömiä.

Yhteenvetona voisi sanoa, että Symantec Mobile Management oli toimintavarma testausalusta, eikä järjestelmässä havaittu suuria puutteita. SMM tarjosi myös hyvät hallintaominaisuudet usealle eri mobiilialustalle. Toivottavasti tulevissa SMM-versioissa varsinkin käyttäjäagenttien tarjoamia ominaisuuksia on kehitetty yhä edelleen. Hallintajärjestelmän yhteensopivuus mobiilaitteiden kanssa oli pääosin hyvällä tasolla. Valitettavasti SMM ei pysty tarjoamaan kaikkia hallintaominaisuuksia jokaiselle käyttöjärjestelmälle. On kuitenkin huomioitava, että ne hallintaominaisuudet, jotka SMM tarjosi, toimivat kiitettävästi.

Testaustulosten ja testauskokemusten perusteella hallintajärjestelmä voidaan mielestäni implementoida viralliseen käyttöön.

LÄHTEET

Alleau, B. & Desemery, J. 2013. Capgemini Consulting. Bring Your Own Device - It's all about Employee Satisfaction and Productivity, not Costs!. Viitattu 5.1.2014 http://www.capgemini-consulting.com/resource-file-access/resource/pdf/bringyourowndevice_29_1.pdf.

Appbrain. 2014. Number of Android applications. Viitattu 20.4.2014 http://www.appbrain.com/stats/number-of-android-apps.

Bond, M. & Landrock, P. 2011. The Trusted Platform Module explained. Viitattu 14.1.2014 http://www.cryptomathic.com/news-events/blog/the-trusted-platform-module-explained.

Campagna, R.; Iyer, S. & Krishnan, A. 2011. Mobile Device Security For Dummies. Hoboken, New Jersey: John Wiley & Sons, Inc.

Chignell, B. 2013. HRZone. The Advantages Of BYOD (Bring Your Own Device). Viitattu 20.2.2014 http://www.hrzone.com/blogs/bchignell/ciphr-blog/advantages-byod-bring-your-own-device.

Citrix 2013. Best practices to make BYOD simple and secure. Viitattu 23.3.2014 https://www.citrix.com/content/dam/citrix/en_us/documents/oth/byod-best-practices.pdf.

Drayton, S. 2013. BusinessZone. The Advantages and Disadvantages of BYOD. Viitattu 25.3.2014 http://www.businesszone.co.uk/blogs/scott-drayton/optimus-sourcing/advantages-and-disadvantages-byod.

Gilmore, G. & Beardmore, P. 2013. Mobile Security & BYOD for dummies, Kaspersky Lab Limited Edition. Viitattu 14.4.2014 http://media.gswi.westcon.com/media/Westcon%20south%20africa/newsletter%20images/August2013/21-BYOD-Dummies.pdf.

Gruman, G. 2014. Windows Phone 8.1 hands-on: The good, the bad, and the ugly. Viitattu 17.4.2014 http://www.infoworld.com/d/mobile-technology/windows-phone-81-hands-the-good-the-bad-and-the-ugly-241748.

Ingraham, N. 2013. The Verge. Apple announces 1 million apps in the App Store, more than 1 billion songs played on iTunes radio. Viitattu 3.5.2014 http://www.theverge.com/2013/10/22/4866302/apple-announces-1-million-apps-in-the-app-store.

Intertek. 2007. Information Security Management Systems ISO 27001. Viitattu 24.5.2014 http://www.certifiering.nu/ecomedia/upload/member/files/611730180611346671545301.pdf.

Juniper Networks. 2011. Mobile device security — Emerging threats, essential strategies. Viitattu 15.5.2014 http://www.adtechglobal.com/data/sites/1/marketing/juniperwhitepapermobiledevicesecurity.pdf.

Litchfield, S. 2012. All About Symbian. Nokia's Asha Touch now 'officially' a 'smartphone' platform. Viitattu 24.4.2014 http://www.allaboutsymbian.com/flow/item/15790_Nokias_Asha_Touch_now_official.php.

Scarfone, K. & Souppaya, M. 2013. Guidelines for Managing the Security of Mobile Devices in the Enterprise. Viitattu 22.04.2014 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf.

Symantec 2014. Implement with One Comprehensive Solution. Viitattu 5.6.2014 http://www.symantec.com/mobility/products.

Teleste 2013. About Teleste. Viitattu 13.2.2013 http://www.teleste.com/about-teleste

Liite 1. Testaustulokset

Testaustuloksissa selvitetään, miten hallintajärjestelmän ominaisuudet ovat toimineet kohdelaitteissa. Tulokset on lajiteltu hallintajärjestelmän testatun ominaisuuden mukaan. Tulokset on myös ominaisuudesta riippuen jaettu eri käyttöjärjestelmiin.

Testaustuloksia tutkiessa on hyvä muistaa, että hallintajärjestelmän testausympäristö ei ole kaikilta osin verrannollinen implementoinnin jälkeiseen käyttöympäristöön. Testausta hankaloittivat sertifikaattiongelmat sekä langattomiin verkkoihin liittyvät rajoitteet. Testaustulokset antavat kuitenkin perustason tietämyksen järjestelmän toimivuudesta.

Salasanan poistaminen kohdelaitteesta (Clear Passcode)

Google Android. Clear Passcode -komento toimi odotetusti Android-pohjaisessa laitteessa. Tämä komento poisti laitteeseen asetetun salasanan/pääsykodin heti, kun komento annettiin. Testauksessa ei havaittu ongelmia.

Apple iOS. Clear Passcode -komento toimi odotetusti Apple iOS -pohjaisessa iPad-tabletissa. Annettu komento poisti laitteeseen asetetun salasanan/pääsykodin heti, kun komento annettiin. Testauksessa ei havaittu ongelmia.

Windows Phone. Hallintajärjestelmä ei tue tätä komentoa Windows Phone -käyttöjärjestelmän laitteissa. Tästä syystä tätä ominaisuutta ei voitu testata Windows Phone -pohjaisilla Lumia 710 ja Lumia 800 -älypuhelimilla.

Symbian. Symbian-käyttöjärjestelmälle ei ole saatavilla käyttäjäagenttia, joten tätä ominaisuutta ei testattu Symbian -pohjaisella Nokia 700 -puhelimella.

Kohdelaitteen etälukitus (Lock Device)

Google Android. Lock Device -komento toimi odotetusti ja lukitsi kohdelaitteen oikeaoppisesti. Komento toimii välittömästi. Testauksessa havaittiin, että jos laitteeseen ei oltu jo ennalta asetettu pääsykoodia, lukitsi tämä annettu komento vain laitteen ruudun.

Apple iOS. Lock Device -komento toimi odotetusti ja lukitsi kohdelaitteen oikeaoppisesti. Komento toimii välittömästi. Testauksessa havaittiin, että jos laitteeseen ei oltu jo ennalta asetettu pääsykoodia, lukitsi tämä annettu komento vain laitteen ruudun.

Windows Phone. Hallintajärjestelmä ei tue tätä komentoa Windows Phone -käyttöjärjestelmän laitteissa. Tästä syystä tätä ominaisuutta ei voitu testata Windows Phone -pohjaisilla Lumia 710 ja Lumia 800 -älypuhelimilla.

Symbian. Symbian käyttöjärjestelmälle ei ole saatavilla käyttäjäagenttia, joten tätä ominaisuutta ei testattu Symbian -pohjaisella Nokia 700 -puhelimella.

Hallintajärjestelmän ja mobiililaitteen hallintayhteyden resetoiminen (Remove MDM and Reset Agent)

Google Android. Komento toimi odotetusti. Kun komento annettiin, poisti se linkin mobiililaitteen ja hallintajärjestelmän väliltä. Testauksessa huomattiin, että jos käyttäjäagentti on auki mobiililaitteessa silloin, kun tämä kyseinen komento annetaan, sulkee se käyttäjäagentti-applikaation välittömästi. Tämän jälkeen käyttäjä joutuu rekisteröimään (enroll) laitteensa uudelleen hallintajärjestelmän kanssa. Testauksessa ei havaittu ongelmia.

Apple iOS. Komento toimi oikeaoppisesti ja välittömästi. Testauksessa ei havaittu ongelmia.

Windows Phone. Hallintajärjestelmä ei tue tätä komentoa Windows Phone -käyttöjärjestelmän laitteissa. Tästä syystä tätä ominaisuutta ei voitu testata Windows Phone -pohjaisilla Lumia 710 ja Lumia 800 -älypuhelimilla.

Symbian. Symbian käyttöjärjestelmälle ei ole saatavilla käyttäjäagenttia, joten tätä ominaisuutta ei testattu Symbian pohjaisella Nokia 700 -puhelimella.

Kohdelaitteen tietojen päivitys hallintajärjestelmään (Send Inventory)

Google Android. Komento lähetti laitteen tiedot ja applikaatiotiedot hallintajärjestelmälle käyttäjäagentin avulla. Testauksessa ei havaittu ongelmia.

Apple iOS. Komento lähetti laitteen tiedot ja applikaatiotiedot hallintajärjestelmälle käyttäjäagentin avulla. Testauksessa ei havaittu ongelmia.

Windows Phone. Hallintajärjestelmä ei tue tätä hallintakomentoa Windows Phone -käyttöjärjestelmän laitteissa. Tästä syystä tätä ominaisuutta ei voitu testata Windows Phone -pohjaisilla Lumia 710 ja Lumia 800 -älypuhelimilla.

Symbian. Symbian käyttöjärjestelmälle ei ole saatavilla käyttäjäagenttia, joten tätä ominaisuutta ei testattu Symbian pohjaisella Nokia 700 -puhelimella.

Laitteen etätyhjennys hallintajärjestelmän avulla (Wipe Device)

Google Android. Wipe Device -komento toimi oikeaoppisesti ja tyhjensi kohdelaitteen välittömästi. Komento tyhjensi kohdelaitteen kokonaan, mukaan lukien applikaatiot ja käyttäjätilit. Testauksessa ei havaittu ongelmia.

Apple iOS. Komento toimi välittömästi ja tyhjensi laitteen datasta, jonka jälkeen kohdelaite käynnisti itsensä uudelleen. Testauksessa ei havaittu ongelmia.

Windows Phone. Hallintajärjestelmä ei tue tätä komentoa Windows Phone -käyttöjärjestelmän laitteissa. Tästä syystä tätä ominaisuutta ei voitu testata Windows Phone -pohjaisilla Lumia 710 ja Lumia 800 -älypuhelimilla.

Symbian. Symbian käyttöjärjestelmälle ei ole saatavilla käyttäjäagenttia, joten tätä ominaisuutta ei testattu Symbian pohjaisella Nokia 700 -puhelimella.

Pääsykoodin pakottaminen kohdelaitteeseen (Set Passcode)

Google Android. Komento toimi oikeaoppisesti ja hallintajärjestelmän kautta voitiin asettaa kohdelaitteeseen pääsykoodi. Kyseinen komento toimi kohdelaitteessa välittömästi. Testauksessa ei havaittu ongelmia.

Apple iOS. Komento toimi oikeaoppisesti ja hallintajärjestelmän kautta voitiin asettaa kohdelaitteeseen pääsykoodi. Kyseinen komento toimi kohdelaitteessa välittömästi. Testauksessa ei havaittu ongelmia.

Windows Phone. Hallintajärjestelmä ei tue tätä komentoa Windows Phone -käyttöjärjestelmän laitteissa. Tästä syystä tätä ominaisuutta ei voitu testata Windows Phone -pohjaisilla Lumia 710 ja Lumia 800 -älypuhelimilla.

Symbian. Symbian käyttöjärjestelmälle ei ole saatavilla käyttäjäagenttia, joten tätä ominaisuutta ei testattu Symbian pohjaisella Nokia 700 -puhelimella.

Mobiililaitteen rekisteröinti hallintajärjestelmään (Enroll)

Google Android. Androidin enroll toimi oikeaoppisesti. Käyttäjäagentissa on valittavissa asetus, jolla voi vaatia SSL:n käyttöä laitteen ja hallintajärjestelmän välillä. Toinen asetusoptio hyväksyy kaikki SSL-sertifikaatit. Käyttäjäagentissa on myös optio merkitä rekisteröitävä laite ”corporate” -statuksella. Jos ”Corporate” -statuksen asetti päälle enrollmentin yhteydessä, näkyi kyseinen laite hallintajärjestelmän inventaariossa merkinnällä ”corporate”. ”Corporate” -statuksen

asettaminen voi olla hyvä keino erotella esim. BYOD- ja yrityksen omistamat laitteet hallintajärjestelmässä. Testauksessa ei havaittu ongelmia.

Apple iOS. iOS-käyttöjärjestelmän enroll toimi oikeaoppisesti. iOS-käyttäjäagentti ei kysynyt enrollin yhteydessä halutaanko laite yhdistää ”corporate” -statuksella hallintajärjestelmään. Testauksessa havaittiin kuitenkin poikkeama EULA-hyväksynnän kanssa. Vaikka EULA:aan oli testausta varten asetettu tekstiä hallintajärjestelmän kautta, näytti iOS-käyttäjäagentti EULA:n täysin tyhjänä. Lisäksi testauksen alkuvaiheessa enroll ei toiminut, koska Applen oman sertifikaatin kanssa oli ongelmia. Ongelma saatiin lopulta ratkaistua ja tämän jälkeen enroll toimi oikeaoppisesti. Applen iOS-käyttöjärjestelmän käyttäjäagentti vaatii SSL-suojattua yhteyttä keskitettyyn hallintajärjestelmään. Testauksessa ei havaittu muita ongelmia.

Windows Phone. Windows Phone -käyttöjärjestelmän laitteen enrollment onnistui vain osittain. Vika oli luultavasti siinä, että Windows Phone tulkitsi SSL-yhteys -sertifikaattia väärin, eikä hyväksynyt sitä oikein. Toinen mahdollinen syy oli testiympäristön langattoman verkkoyhteyden tiukat palomuuriasetukset. Testilaite kuitenkin onnistuttiin yhdistämään hallintajärjestelmään käyttämällä mobiililaitteen datayhteyttä tai toista Wi-Fi-verkkoa. Enrollment onnistui vain osittain ja tämä huomattiin esimerkiksi siitä, että laitteen käyttäjäagentin ja hallintajärjestelmän välinen yhteys katosi ajoittain.

Windows Phone -käyttöjärjestelmän kanssa oli enrollmentin kanssa suurimmat ongelmat. Testitapauksessa havaittiin ongelmia.

Symbian. Symbian käyttöjärjestelmälle ei ole saatavilla käyttäjäagenttia, joten tätä ominaisuutta ei testattu Symbian -pohjaisella Nokia 700 -puhelimella.

Hallintajärjestelmän sovelluskirjasto (Mobile Library)

Hallintajärjestelmän sovelluskirjaston avulla testattiin, miten erilaiset objektit eli Item:it toimivat itse hallintajärjestelmässä sekä mobiililaitteissa. Kun sovelluskirjastoon lisätään objekti, ilmestyy se hallittavien mobiililaitteiden käyttäjäagentti-

en kirjastoon eli libraryyn. Librarysta käyttäjä voi ladata näitä objekteja mobiililaiteeseensa.

Tässä testitapauksessa käytettiin seuraavia tiedostotyyppejä (Taulukko 2). Taulukossa OK-tulos tarkoittaa, että kyseinen objekti toimi hyvin valitussa käyttöjärjestelmässä. NOK-tulos tarkoittaa sitä, että kyseinen objekti ei syystä tai toisesta toiminut kunnolla kohteena olevassa käyttöjärjestelmässä. Yleisin syy NOK-tulokselle oli yksinkertaisesti se, että mobiililaitteen käyttöjärjestelmä ei tukenut kyseistä tiedostotyyppiä.

Itemien lisäksi Mobile Libraryyn liittyvät olennaisena osana feedit. Feedit ovat ns. sisältövirtoja, joihin Item-objekteja voidaan lisätä. Feedit antavat paljon myös joustovaraa asetusten suhteen. Yksi feed voi keskittyä esimerkiksi applikaatioiden jakamiseen ja toinen esim. html-tiedotteiden jakamiseen. Feedit voi myös jakaa kohdelaitteen käyttöjärjestelmässä käytetyn kielen mukaan.

Taulukko 2. Mobile Library -objektien tulokset mobiililaitteissa.

		Google Android	Apple iOS	MS Windows Phone
Videotiedostot	.avi	NOK	NOK	NOK
	.mpeg4	NOK	NOK	NOK
	.wmw	NOK	NOK	NOK
Musiikkitiedostot	.mp3	OK	OK	NOK
	.flac	NOK	NOK	NOK
Tekstitiedostot	.doc	OK	OK	OK
	.odt	NOK	NOK	NOK
	.txt	OK	OK	OK
Taulukkotiedostot	.xls	OK	OK	OK
	.ods	NOK	NOK	NOK
Kuvatiedostot	.jpg	OK	OK	OK
	.gif	OK	OK	OK
HTTP-linkki	.http	OK	OK	OK

Vaikka eri tiedostotyypit toimivat vaihtelevasti mobiililaitteissa, on kuitenkin otettava huomioon, että itse Mobile Library toimi kiitettävästi. Feedien luominen ja objektien lisääminen oli tehty helpoksi ja virtaviivaiseksi. Ongelmat liittyivät lähinnä mobiililaitteen ja hallintajärjestelmän väliseen yhteyteen.

Isoimmat ongelmakohdat tulivat vastaan Windows Phone -käyttäjäagentin kanssa. Käyttäjäagentti hävitti välillä libraryn objekteja ja ongelma korjautui yleensä sillä, että kyseisen mobiililaitteen rekisteröi (enroll) uudestaan hallintajärjestelmään. Ongelmaa ei saatu täysin selvitettyä, vahvana veikkauksena oli tapa, jolla Windows Phone käsittelee sertifikaatteja. Tämän takia Windows Phone -käyttäjäagentin ja hallintajärjestelmän välinen yhteys saattoi katkeilla. Toinen syy saattoi olla testiympäristön langattomien verkkojen tiukat palomuuriasetukset. Testausta pystyttiin kuitenkin ongelmatapauksissa suorittamaan mobiililaitteen datayhteydellä tai toisella Wi-FI-verkkoyhteydellä.

Symbian. Symbian käyttöjärjestelmälle ei ole saatavilla käyttäjäagenttia, joten tätä ominaisuutta ei testattu Symbian pohjaisella Nokia 700 -puhelimella.

Jailbreak ja rootatut laitteet

Tässä testitapauksessa oli käytössä yksi rootattu laite (ZTE Blade).

Google Android. SMM tunnisti ZTE Blade -älypuhelimen rootatuksi, kun laitteella suoritettiin hallintajärjestelmään rekisteröinti (enroll). Laite näkyi SMM inventaariossa ja sai merkinnän ”JAILBROKEN” roottauksen johdosta. SMM 7.2 MR1 -järjestelmäversiossa rootatulle laitteelle ei voinut suorittaa mitään laitehallinnan komentoja. SMM 7.2 SP1 -järjestelmäversiossa on mahdollista hyväksyä rootattu laite hallintaan. Tätä ominaisuutta testattiin ja se toimi hyväksytysti. Rootatun laitteen hyväksymisen jälkeen laite käyttäytyi kuin normaali hallittava Android-laite.

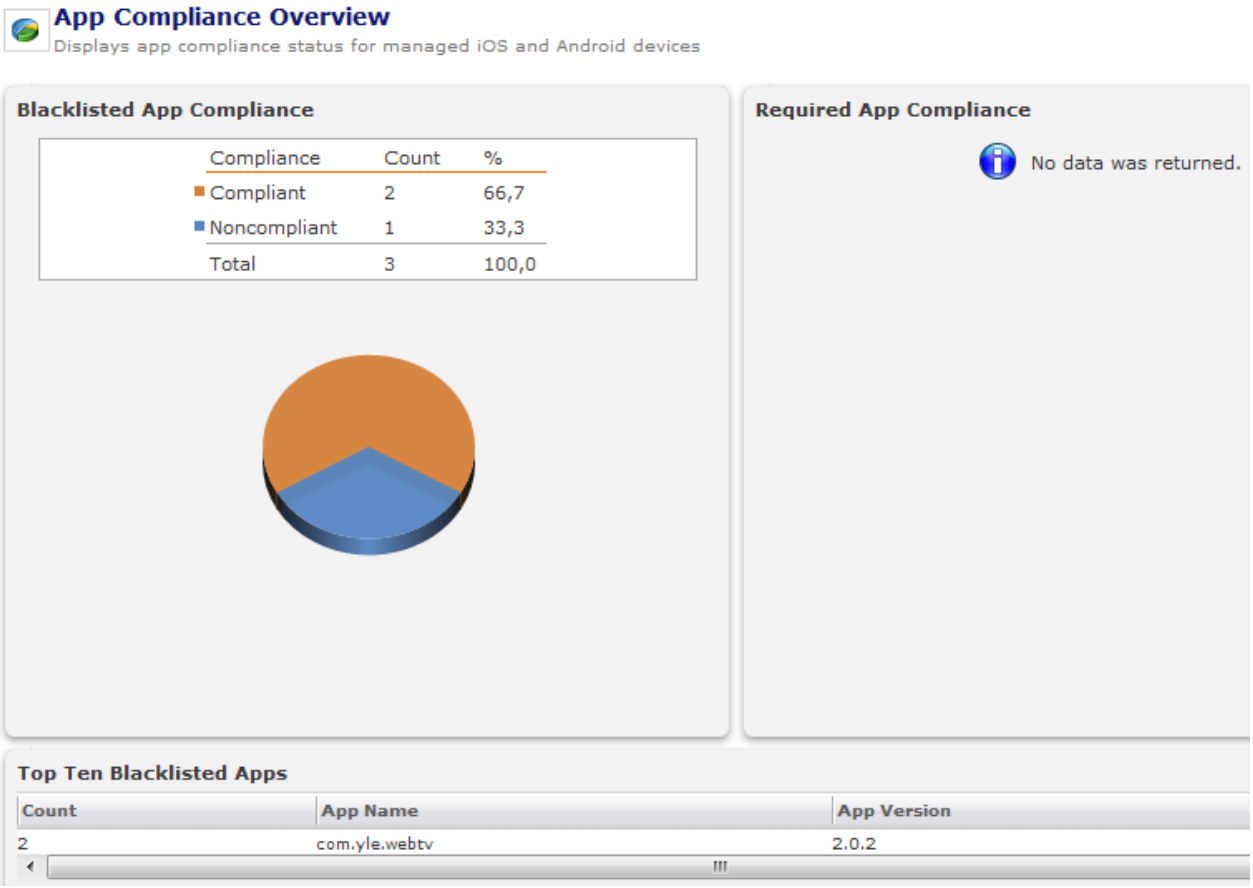
Apple iOS. SMM tunnisti iOS jailbreak -laitteet, mutta tässä testiprojektissa ei ollut mahdollista kokeilla jailbreakin vaikutuksia hallintajärjestelmään. Testiprojektissa käytetty iPad oli testauksen aikana käytössä myös muissa työtehtävissä. Tämän takia jailbreakia ei voinut kyseiselle laitteelle tehdä.

Windows Phone. Tämä testitapaus ei koske Windows Phonea.

Symbian. Tämä testitapaus ei koske Symbiania.

Applikaatioiden kieltolista (Application Blacklisting)

Application Blacklisting -ominaisuutta varten luotiin uusi sääntö testikäyttöön. Tässä testisäännössä määritettiin Yle Areena -applikaatio kielletyksi sovelluksiksi. Testitapauksessa kyseinen kielletty applikaatio ladattiin useaan mobiililaitteeseen ja tämän jälkeen päivitettiin mobiililaitteen laitetiedot ja inventaario hallintajärjestelmään. Lähetetyt tiedot ja inventaario olivat siirtyneet hallintajärjestelmään ja järjestelmä tunnisti kyseisen asennetun Yle Areena -applikaation ”kielletyksi” (Kuva 10). Testitapaus onnistui hyväksytyksi.



Kuva 10. Blacklisted Apps -statistiikkaa.

Exchange ActiveSync -ominaisuudet ja käyttöpolitiikka (Policy)

Google Android. Android-käyttöjärjestelmällä testattiin esimerkiksi Exchange ActiveSync -ominaisuutta määrittää pääsykoodin vaatimukset. Politiikkaan asetettiin, että pääsykoodi on vähintään 5 merkkiä pitkä ja että laite lukitsee itsensä (lock screen) 20 sekunnin jälkeen. Politiikka saatiin asetettua kohdelaitteeseen onnistuneesti ja asetetut pääsykoodin vaatimukset pysyivät voimassa. Testitapaus onnistui hyväksytysti.

Androidilla on myös mahdollista konfiguroida Touchdown-applikaation avulla erittäin monipuolisia käyttöpolitiikka-asetuksia. Touchdown on monipuolinen sähköpostisovellus, joka on kehitetty yritysten käyttöön. Testitapauksessa yritettiin luoda Touchdown-käyttöpolitiikka ja asettaa se kohdelaitteeseen. Käyttöpolitiikan asettaminen ei kuitenkaan onnistunut, koska Touchdown-applikaation sähköpostiasetuksia ei saatu toimimaan. Tämä testitapaus epäonnistui.

Apple iOS. iOS-käyttöjärjestelmän kanssa suoritettiin esimerkiksi testitapaus, jossa määritettiin laitteen pääsykoodin pituus. Politiikka yritettiin asettaa testattavaan kohdelaitteeseen, mutta politiikka-asetus ei mennyt laitteelle saakka. Syyksi epäiltiin jälleen kerran sertifikaatteihin liittyviä ongelmia. Testitapaus epäonnistui.

Windows Phone. Windows Phone -käyttöjärjestelmän kanssa testattiin Exchange ActiveSyncin Device Wipe -ominaisuutta, joka tyhjentää kohdelaitteen. Testilaitteeseen syötettiin matti.mouho:n käyttäjätunnukset sekä sähköpostiosoite. Tämän jälkeen laitteelle lähetettiin EAS Device Wipe -komento, joka tyhjensi laitteen onnistuneesti.

Symbian. Symbian -pohjainen Nokia 700 oli tämän testiprosessin ainoa mobiililaite, johon ei ole saatavilla natiivia käyttäjäagenttia. Symbian-pohjaisen laitteen hallinta täytyy toteuttaa kokonaisuudessaan Exchange ActiveSyncin avulla.

Nokia 700 puhelimella Exchange ActiveSyncin vaatima sähköposti konfiguroitiin puhelimen omalla Mail for Exchange -sovelluksella. Nokia 700 -puhelimelle tehtiin testikäyttöä ajatellen käyttöpolitiikka, jossa kiellettiin laitteen kameran ja

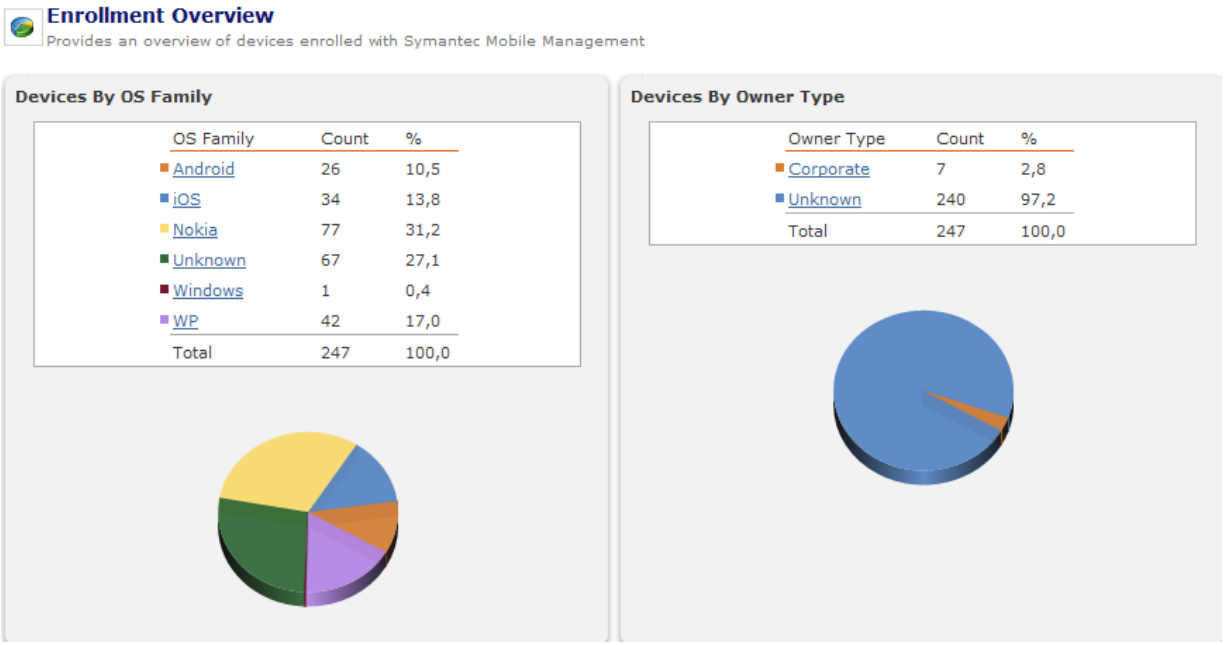
Bluetooth-yhteyden käyttö. Testitapauksessa havaittiin, että kohdelaite ilmoitti, että kyseinen politiikka oli saapunut laitteeseen ja sen voi joko hyväksyä tai hylätä. Testitapauksessa politiikka tietysti hyväksyttiin. Hyväksymisen jälkeen yritettiin käyttää mobiililaitteen kameraa ja Bluetooth-yhteyttä, mutta laite näytti, että nämä ominaisuudet on poistettu käytöstä (Disabled).

Asia toimii myös käänteisesti. Jos politiikassa määritetään, että esimerkiksi nämä ominaisuudet on sallittu, tulee siitäkin laitteeseen pop-up ilmoitus (esim. Enabled: Bluetooth, camera). Testitapaus onnistui hyväksytysti.

Hallintajärjestelmän raportointityökalut

SMM tarjoaa kattavat raportointi- ja tilastointiominaisuudet laitteiden hallinnantaan. Esimerkiksi hallintajärjestelmän avulla on mahdollista tutkia laitteiden käyttöjärjestelmien prosenttiosuuksia (Kuva 11). Tilastoja ja graafeja löytyy myös laitelisensseistä, käytetyistä applikaatioista jne.

Järjestelmä mahdollistaa myös raporttien tulostamisen tai tallentamisen esimerkiksi taulukkomuotoisena. Testitapauksessa otettiin raportti mobiililaitteiden lukumääristä käyttäjineen ja laitenimineen jne. Raportit saatiin ulos csv-taulukkomuodossa sekä html-muotoisena. Raporttien ulkomuoto ja datan paikkansapitävyys olivat kunnossa. Testitapaus onnistui hyväksytysti.



Kuva 11. Tilasto käyttöjärjestelmien prosenttiosuuksista.