Wille Tuovinen

Fysiologisiin mittauksiin käytettävien laitteiden etähallinta ja -seuranta

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikan tutkinto-ohjelma

Insinöörityö

10.11.2021

Tiivistelmä

Tekijä:	Wille Tuovinen
Otsikko:	Fysiologisiin mittauksiin käytettävien laitteiden etähallinta ja -seuranta
Sivumäärä:	31 sivua
Aika:	10.11.2021
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Ammatillinen pääaine:	Hyvinvointi- ja terveysteknologia
Ohjaajat:	Yliopettaja Mikael Soini Teknologiajohtaja Otto Teinonen

---

Mobiililaitteiden hallinnan ja seurannan tärkeys on kasvanut viimeisen kymmenen vuoden aikana merkittävästi. Mobiililaitteet sisältävät yhä henkilökohtaisempaa ja työelämään liittyvää tietoa. Seuraamattoman ja hallitsemattoman tiedon lisääntyminen kasvattaa tietoturvariskejä, joiden seuranta ja hallinta jäävät yleisesti loppukäyttäjän vastuulle. Tämä voi aiheuttaa riskitilanteen, jossa tiedon päätyminen julkisuuteen tai varkaan käsiin on vain ajan kysymys.

Insinöörityön tavoitteena on kartoittaa, testata ja löytää MDM (Mobile Device Management) -ratkaisu, jolla kyettäisiin saavuttamaan Insinöörityön tilaajan Medixine Oy:n asettama tavoite saada MDM-ratkaisu tuotantokäyttöön vuoden 2021 loppuun mennessä.

Työn edetessä jouduttiin toteamaan, että turvallisuusasetusten tutkimiseen ja käyttöönottoon tulee projektissa keskittyä enemmän. Insinöörityön tuloksena saatiin Medixinen asettamiin vaatimuksiin perustuen testattua ja löydettyä potentiaalisin MDM-ratkaisu. Insinöörityöosuuden jälkeen käytännön toteutus jatkuu, ja tavoitteena on saada MDM-ratkaisu tuotantokäyttöön vielä tämän vuoden puolella.

Työn tuloksia voidaan käyttää hyväksi tilanteessa, jossa organisaatiolla on tarvetta ottaa käyttöön mobiililaitteidenhallinnalle tarkoitettu palvelu eikä alustavaa tietoa ja ymmärrystä ole palveluun liittyen.

Avainsanat: Mobile Device Management, Mobile Application Management, Android, Microsoft Intune, Sophos Mobile

Abstract

Author:	Wille Tuovinen
Title:	Remote Control and Monitoring of Equipment Used for Physiological Measurements
Number of Pages:	31 pages
Date:	10 November 2021
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communication technology
Professional Major:	Health Technology
Instructors:	Mikael Soini, Principal lecturer Otto Teinonen, Chief Technology Officer

---

The importance of mobile device management and monitoring has grown significantly over the last ten years. Mobile devices increasingly contain more personal and work-related information. The increase in unmonitored and unmanaged information adds to security risks The monitoring and management of information is generally the responsibility of the end user. This can lead to a risk situation where the information ends up in the public domain or in the hands of a thief.

The goal of the study was to map, test and find an MDM (Mobile Device Management) solution that would achieve the goal set by Medixine Oy, the commissioner of the study, and to get the MDM-solution into production use by the end of 2021.

As the study progressed, it had to be stated that the project should focus more on researching and implementing the security settings. As a result, the most potential MDM-solution option was tested and found within the requirements set by Medixine. The practical implementation of the solution will continue after having finished the thesis and the goal is to get the MDM-solution into production use later this year.

The results of the study can be used in a situation where the organization needs to implement a service for mobile device management and there is no preliminary knowledge and understanding of the service.

Keywords: Mobile Device Management, Mobile Application Management, Android, Microsoft Intune, Sophos Mobile

Sisällys

Lyhenteet

AD: *Active Directory*. Active Directory on Microsoftin Windows-toimialueen käyttäjätietokanta ja hakemistopalvelu, jonka avulla vodaan hallita yrityksen laitteita, käyttäjiä ja verkon resursseja.

API: Application Programming Interface. API on suomennettuna sovellusohjelmointirajapinta, joka on ohjelmointiliitäntä, jonka avulla kaksi sovellusta voivat keskustella toistensa kanssa.

BT/BLE: *Bluetooth tai Bluetooth low energy*. Näillä tarkoitetaan lyhyen kantaman radiotekniikkaan perustuvaa langatonta tiedonsiirtotekniikkaa, joka mahdollistaa hyvin vähäisellä energiankulutuksella toteutettavan tiedonsiirron. Bluetooth low energy (BLE) eroaa perinteisestä Bluetoothista (BT) siten, että BLE yksinkertaisesti käyttää huomattavasti vähemmän energiaa tiedonsiirron toteuttamiseen, josta se saa nimensäkin.

EKG: *Elektrokardiogrammi.* Sydänsähkökäyrä (EKG) on testi, jota voidaan käyttää sydämen rytmin ja sähköisen aktiivisuuden tarkistamiseen.

GUI: *Graphical User Interface*. Suomeksi graafinen käyttöliittymä on interaktiivisten visuaalisten komponenttien järjestelmä tietokoneohjelmistoille. GUI näyttää objektit, painikkeet ja kuvat, jotka välittävät tietoja ja edustavat toimintoja, jotka käyttäjä voi tehdä.

IoT: *Internet of Things.* Esineiden internet tarkoittaa järjestelmää, joka perustuu teknisen laitteen suorittamaan automaattiseen tiedonsiirtoon.

MAM: *Mobile application management*. Mobiilisovellusten hallinta (MAM) viittaa jokaisen yrityksessä käytetyn sovelluksen koko elinkaaren

hallintaan, mukaan lukien sovellusten asentaminen, päivittäminen ja poistaminen sekä yrityksen omilla laitteilla, että organisaatiossa.

MDM: *Mobile device management*. Tällä tarkoitetaan mobiililaitteiden, kuten älypuhelinten, taulutietokoneiden ja kannettavien tietokoneiden hallintaa.

MTD: *Mobile Threat Defense*. Tällä tarkoitetaan ratkaisua, jolla on valmiudet suojata mobiililaitteita, alustoja, sovelluksia ja verkkoja useilta yleisiltä ja edistyneiltä uhilta.

QR-koodi: *Ruutukoodi.* Ruutukoodilla tarkoitetaan kaksiulotteista kuviokoodia, johon on koodattu informaatiota. QR-koodin voi lukea matkapuhelimeen ladatulla siihen tarkoitetulla sovelluksella tai käyttöjärjestelmän sisään rakennetulla lukuominaisuudella.

SaaS: *Software as a Service*. SaaS on palvelu, jolla tarkoitetaan pilvessä sijaitsevaa ohjelmistoa, jota ylläpidetään palveluntarjoajan toimesta. SaaS-palvelut välitetään verkkoselaimen kautta, sovelluksena tai näiden hybridinä.

SMS: *Short Message Service.* Matkapuhelinten tekstiviestijärjestelmä. Toisin sanoen tekstiviesti.

UEM: *Unified Endpoint Mangement*. Suomeksi yhdenmukaistettu päätelaitteiden hallinta, joka yhdistää monia muita tekniikoita hallita, seurata ja turvata laitteita ja sovelluksia.

1 Johdanto

2000-luvun alussa mobiililaitteiden käyttö alkoi lisääntyä yrityksissä. Siitä lähtien se on kasvanut tasaisesti ja mobiililaitteista on tullut olennaisia työkaluja nykypäivän työpaikoilla. Mobiililaitteet lisäävät joustavuutta ja tuottavuutta, mutta kun niitä ei hallita, ne voivat asettaa erilaisia haasteita organisaatioille. Mobiililaitteiden hallinnan ja näkyvyyden puuttuminen voi aiheuttaa tehottomuutta ja tietoturvariskejä. Mobiililaitteiden hallinta (MDM) on hyvä tapa luoda perusta yritysten hallussa olevien mobiililaitteiden tietoturvastatuksen seurannalle. MDM on mobiililaitteiden etähallinta ja -seurantapalvelu, joka on yrityksille hankittavissa palveluntarjoajilta. MDM on yleisimmin toteutettuna web-pohjaisena pilvipalvelusovelluksena. (1.)

Mobiililaitteiden etähallinta on vuosikymmenen sisällä noussut yhdeksi tärkeimmäksi kehityskohdaksi tekniikan ja tietoturvan kehityksen saralla. Useimmilla aloilla etätyöskentely on lisääntynyt räjähdysmäisesti, ja sen seurauksena yritysmaailman mobiililaitteiden käyttö on monipuolistunut. Mobiililaitteissa olevan arkaluonteisen tiedon määrä on lisääntynyt ja siksi on yhä tärkeämpää tuntea ja ymmärtää tiedon ja mobiililaitteiden hallintaa. Tähän perustuen erityisesti tietoteknistenlaitteiden käyttöturvallisuuden tulisi olla entistä parempaa. Mobiililaitteiden tulisi olla tarpeen tullen hallittavissa ja seurattavissa, ei vain tiedon, vaan myös laitteiden ja ohjelmiston osalta. (1; 2.)

Insinöörityön aiheena on tutkia, kartoittaa ja löytää MDM-ratkaisu, jolla saadaan toteutettua Medixinen tarjoamien fysiologisiin mittauksiin käytettävien laitteiden etähallinta ja -seuranta. Insinöörityön aikana tulee jatkuvasti pitää mielessä MDM-ratkaisun löytämiselle asetetut vaatimukset, jotta vältyttäisiin työlle suunnitellun työajan haaskaamiselta.

2 Medixine Oy

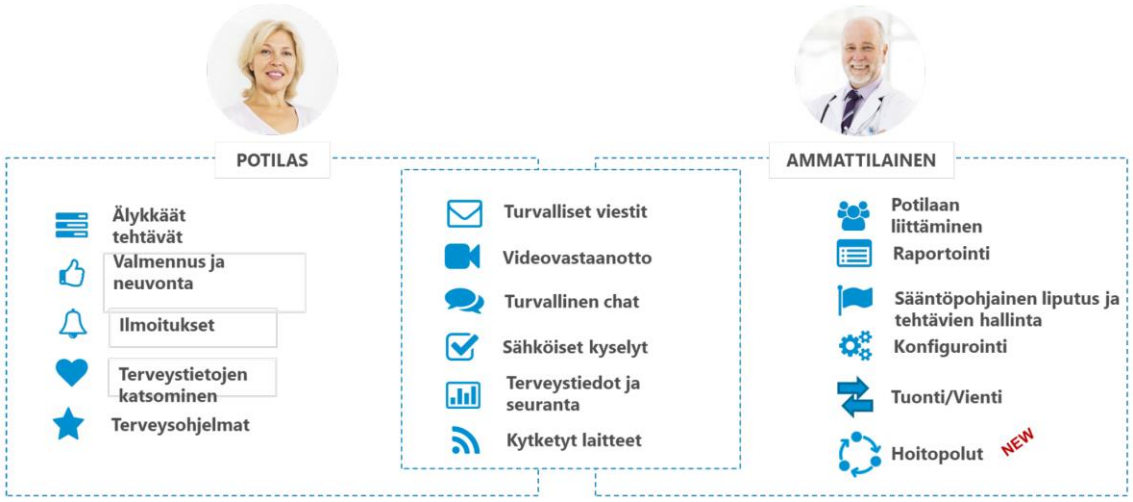
2.1 Medixine sovellustalona

Medixine Oy on terveysteknologia-alan sovellustalo, joka kehittää, markkinoi ja myy etälääketieteen (telehealth) kokonaisvaltaista alustaratkaisua (3). Medixine työllistää vuonna 2021 kaksikymmentäyksi alan ammattilaista, joiden taustalta löytyy tekniikan ääripäiden oppineita, tohtorikoulutuksen omaavia terveydenalan ammattilaisia, sekä myös myynnin ja markkinoinnin parhaimmistoa. Medixinen yhtenä lähitulevaisuuden suurimpina tavoitteina on päästä levittämään terveysteknologian SaaS (Software as a Service) -ratkaisuaan jo osittain vallatun Euroopan markkinan lisäksi myös Amerikan markkinoille.

2.2 Medixine Suite

Medixine Suite on pilviohjelmisto terveydenhuoltoalan yrityksille. Se on joustava, verkkopohjainen viestintäratkaisu, joka on erityisesti suunniteltu auttamaan ammatillista hoitoryhmää kehittämään ja toteuttamaan valmennus- ja hoito-ohjelmia, seuraamaan hoidettavasta saatuja fysiologisia mittausarvoja, sekä yksilöiden että väestön edistymistä ja tarjoamaan automatisoitua, henkilökohtaista palautetta hoidettaville ja valmennettaville etäyhteyden kautta. Medixine Suite on suunniteltu pitämään yksityishenkilöt yhteydessä terveydenhuollon tiimin kanssa, mukaan lukien omaishoitajat, valmentajat ja ystävät, kaikki turvallisessa, suljetussa ympäristössä (4). Medixine Suiten osalta insinöörityössä keskitytään ominaisuuteen vastaanottaa mobiililaitteelta lähetettäviä fysiologisia mittausarvoja. Medixinen ratkaisu perustuu omaan teknologiaan, jota voidaan käyttää kaikilla yleisimmillä päätelaitteilla. Medixine Suite voidaan tarjota asiakkaille niin pilvialustalle asennettuna kuin omana on-premise asiakasprojektikohtaisena asennuksena. On-premisellä tarkoitetaan asiakkaan fyysisesti itse ylläpitämää web-palvelinta, jolle Medixine Suite voidaan asentaa. Medixine Suite tarjoaa SaaS-ratkaisuna useita valittavissa olevia niin sanottuja moduuleja (5). Kuvassa 1 on esitetty Medixine Suiten

ominaisuuksia (moduuleja), jotka ovat räätälöitävissä käyttöön tai pois asiakaskohtaisten toiveiden mukaan. (5.)



Kuva 1. Medixine Suiten ominaisuudet paloiteltuna.

Kuvassa 1 on esitetty Medixine Suiten ominaisuudet terveydenhuollon ammattilais- ja potilaskäyttäjäkohtaisesti.

Medixine Suitessa on terveydenhuollon ammattilaiselle tarjolla monipuoliset työvälineet viestinnän ja seurannan toteuttamiseksi. Medixine Suiten ominaisuuksiin kuuluvat turvallinen chat-toiminto, videovastaanotot, viestit ja myös sähköiset kyselyt. Lisäksi hoitohenkilökunnan työajan säästämiseksi alustalla on myös tarjolla etäseurantatoiminto ja automaattinen potilaiden seulonta.

Yhtiön viimeisen kahdenkymmenen vuoden kehityksen tuloksena syntynyt tuote vastaa juuri nyt markkinoiden voimakkaaseen kysyntään. Tuote tukee asiakkaiden tarpeita ja antaa Medixinelle uniikin kilpailuaseman terveysteknologian sovellusmarkkinoilla. Koronaviruksen ilmaantuessa maailmanlaajuiseksi epidemiaksi koronaviruspesifejä tilauksia alkoi ilmestyä asiakastilauslistoille runsain määrin, jotka vauhdittivat vuoden 2020 yritystoimintaa (6). Maailman koronavirustilanteen normalisoituessa koronaviruksen torjuntaan käytettävien palveluiden kysyntä laskee, mutta

etähoitoon tottuneiden asiakkaiden voi odottaa edelleen lisäävän muiden tuotantovalmiiden ratkaisujen kysyntää.

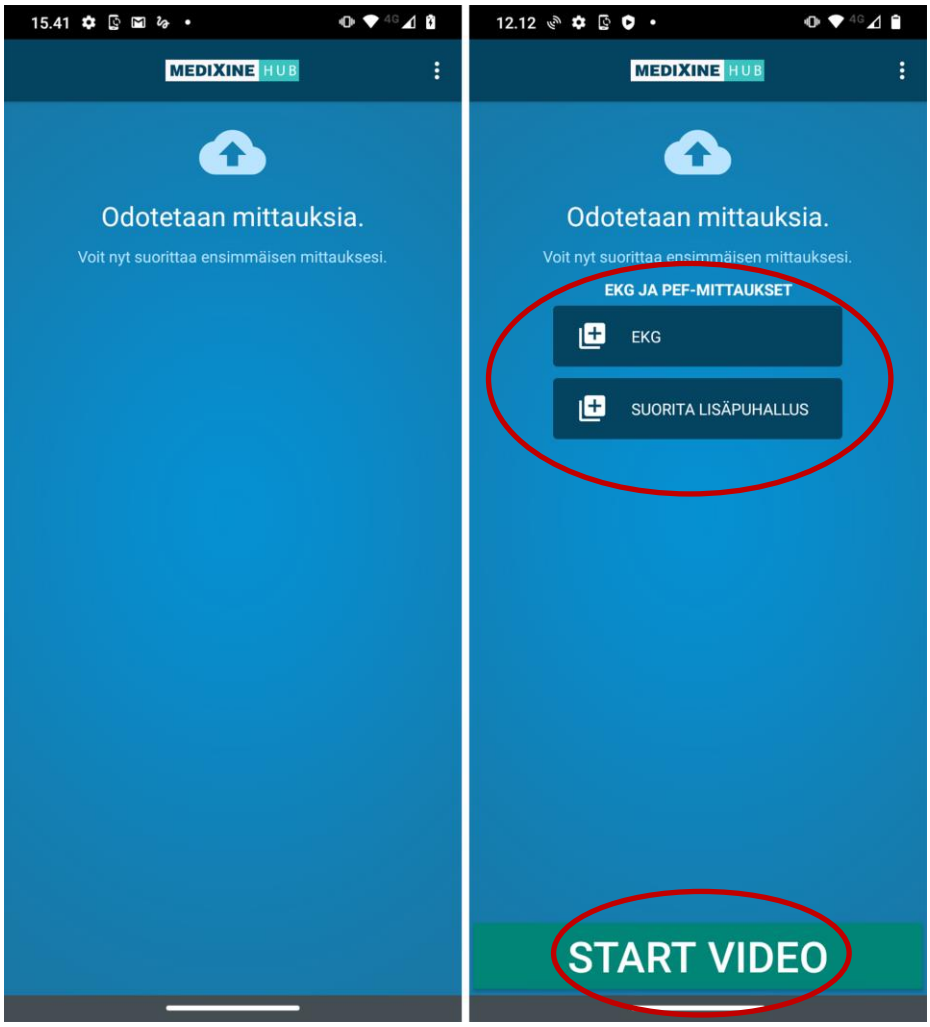
2.3 Medixine DeviceHub

2.3.1 Mobiilisovelluksen tarkoitus ja käyttö

Medixine DeviceHub on Android-pohjainen mobiilisovellus, jonka tarkoituksena on prosessoida mobiililaitteen vastaanottamia fysiologisia mittausarvoja. Kun mittaus on saapunut mobiililaitteeseen asennettuun DeviceHub-sovellukseen, tämä lähettää saadut arvot parametreineen Medixine Suite -web-sovellukseen. Medixine DeviceHub tulee konfiguroida lähettämään sen saamat mittausarvot oikeaan kohteeseen (asiakaskohtainen Medixine Suite). Vaikka taustalla onkin valmis mobiilisovellus, useat asiakkaat toivovat asiakaskohtaisia räätälöintejä, eli asiakkaan toiveesta toteutettavia lisäominaisuuksia, jotka ovat pääsääntöisesti tehty GUI (Graphical User Interface) -puolelle. Näillä voidaan tarkoittaa esimerkiksi asiakkaan toivomaa lisämittauspainiketta, tai vain yksinkertaista sovelluksen taustavärin muutosta. Tulevaisuudessa suunnitelmissa on mahdollistaa sovelluksen kautta myös videovastaanottoja ammattilaisen ja potilaan välillä.

Medixine DeviceHub on toteutettu käytön helppous edellä, joten loppukäyttäjän, jonka luona mobiililaite sijaitsee, ei mittausta ottaessa tarvitsisi lainkaan olla kosketuskontaktissa DeviceHub-sovelluksen sisältämään mobiililaitteeseen. Oletuksena on, että potilas toteuttaa mittalaitteella mittauksen ja DeviceHub-mobiilisovellus ilmaisee äänimerkillä, kun mittaus on onnistuneesti vastaanotettu, käsitelty DeviceHub-sovelluksessa ja lähetetty Medixine Suite web-sovellukseen. Medixine DeviceHubin GUI on suunniteltu mahdollisimman yksinkertaiseksi. Se on suunniteltu käyttäjäystävällisyys etusijalla, jotta iästä tai teknisestä osaamisesta riippumatta sen käyttö on helppoa. Kuvan 2 vasemmalla puolella on nähtävissä DeviceHubin GUI oletuskokonaisuutena.

Oikealla puolella on nähtävissä DeviceHub asiakasprojektispesifillä videovastaanottopainikkeella ja muutamalla lisäpainikkeella varustettuna.



Kuva 2. Medixine DeviceHub GUI -oletuskokonaisuus vasemmalla ja oikealla lisätoiminnallisuuksilla (punaisella ympyröity).

2.3.2 DeviceHub-historiaa

Medixine DeviceHub -etämonitorointiratkaisun historia menee kauas yli kymmenen vuoden päähän. Myös ensimmäiset etämittausratkaisut tuotiin markkinoille yli kymmenen vuotta sitten. Ratkaisu perustui Nokian älypuhelinten BT/BLE (Bluetooth tai Bluetooth low energy) -kyvykkyyksiin ja mittaustietojen välittämiseen palvelimelle SMS (Short Message Service) -viestillä. Tänä päivänä on päädytty ratkaisuun, jossa puhelinmalli valitaan asiakasyrityksen puolesta, vaikka teoriassa DeviceHub-mobiilisovellus toimii kaikissa Android-pohjaisissa mobiililaitteissa. Android-versioilla ja mittauslaitteilla on suuri

vaikutus sovelluksen toimintojen toimimiseen. Esimerkiksi vuonna 2018 eräälle asiakasyritykselle julkaistiin pilotti, jossa ei osattu varautua mobiili- ja mittauslaitteen välisessä BT-yhteydessä kohdattuihin yllättäviin ongelmiin. Tässä tapauksessa mobiililaite ilman selvää syytä katkaisi yhteyden mobiililaitteen ja mittauslaitteen väliltä, ja toimitetut mobiililaitteet jouduttiin vaihtamaan toiseen malliin. (4.)

2.4 Medixinen lähivuosien tavoitteet

Medixinen tämänhetkisten asiakassopimusten piirissä on yli 2,5 miljoonaa loppukäyttäjää. Tuote on käytössä kuudessa eri Euroopan maassa, mm. Suomessa, Tanskassa, Isossa-Britanniassa ja Espanjassa. Viime aikoina on haviteltu myös Amerikan mantereelta potentiaalisia asiakkaita.

Medixinen viime vuosien saavutuksiin kuuluu useita merkittäviä asiakkuuksia. Näitä ovat esimerkiksi Nestle Health Sciences / Vitaflo, Aetna, NHS, Linde, YTHS, IEM ja useita Tanskassa sijaitsevia sairaalayksikköjä. Medixinen myynnin kauppojen kokonaisarvo on 7,0 M€ 1.8.2021 ja allekirjoitettujen sopimusten arvo on laskettu olevan seuraavalle kymmennelle vuodelle jopa 7,0 M€. (7.)

Vuonna 2020 Medixine sai kerättyä 2,9 miljoonan euron rahoituskierroksen, josta suurin osa koostui Springvestin järjestämästä joukkorahoituskampanjasta. Medixinen tavoitteena on käyttää rahoitusta kasvattaakseen kansainvälistä liiketoimintaansa lähinnä Isossa-Britanniassa ja Keski-Euroopassa. Lisäksi tavoitteena on kohdistaa saatuja resursseja uusien tuotteiden kehitykselle. (8.)

2.5 Liikevaihto ja tavoitteet

Euroopan etälääketieteen (telehealth) markkinoiden on ennustettu kasvavan vuoden 2021 USD 11,32 miljardista USD 21,80 miljardiin 14 % vuoteen 2026 mennessä (9). Koronavirusepidemian aikana tapahtuneet maailmanmarkkinoiden muutokset ovat kuitenkin vaikuttaneet kasvuun ja

lähitulevaisuudessa toteutuvat luvut voivat huomattavasti poiketa ennusteesta. Euroopan etälääketieteen markkinat ovat erittäin voimakkaassa nousussa, ja Medixinellä on todellinen mahdollisuus varmistaa merkittävä markkinaosuus lyhyessä ajassa (7). Taulukossa 1 esitetään kahden tulevan vuoden liikevaihtoennuste. (5.)

Taulukko 1. Medixinen liikevaihdon lähitulevaisuuden ennuste.

	2017	2018	2019	2020	2021	2022	2023
Lisenssimyynti & SaaS	100 000 €	800 000 €	1 246 000 €	1 380 000 €	3 000 000 €	6 020 000 €	13 800 000 €
Projektimyynti	800 000 €	700 000 €	600 000 €	700 000 €	500 000 €	700 000 €	1 150 000 €

Medixinen lähitulevaisuuden liikevaihtoennuste seuraavalle kahdelle vuodelle näyttää lupaavalta. Yrityksen viime vuoden aikana toteuttamat henkilöstöpalkkaukset ja loppuvuodesta 2021 toteutuva muutto modernimpaan toimistoympäristöön vahvistavat entuudestaan yrityksen vahvaa kasvua alan markkinoilla. (8.)

3 Insinöörityössä käytettävät teknologiat

3.1 Mobiililaitteet

Mobiililaitteet mittausarvojen vastaanottamiseksi ja niiden lähettämiseksi BT/BLE-tekniikkaa hyväksi käyttäen ovat tällä hetkellä vielä rajoittuneet Android-käyttöjärjestelmän sisältäviin mobiililaitteisiin. Toisin sanoen vastaanottavana laitteena voi olla käytössä esim. matkapuhelin, taulutietokone (tablet) tai jokin muu vastaava laite. Medixinellä mobiililaitteet on valittu tähän mennessä edullisen hinnan perusteella, sillä Medixine DeviceHub ei vaadi käytettävältä laitteelta juurikaan prosessointitehoja. Ennen lopullista laitteen valintaa tulee sopivuus testata kaikki mahdolliset tilanteet huomioon ottaen. Taustaosiossa jo mainitussa BT/BLE-tekniikan kanssa kohdatut ongelmat huomioon ottaen, tulee testata jokainen Medixinen ilmoittama yhteensopiva laite

useaan kertaan ja laaja-alaisesti. Tällä kartoitetaan pois mahdolliset mitta- ja mobiililaitteiden väliset ongelmatilanteet.

3.2 Fysiologisiin mittauksiin käytettävät mittauslaitteet

Medixinen tuetut mittalaitteet, joita käytetään fysiologisten mittausarvojen mittaamiseksi, ovat verenpainemittari, happisaturaatiomittauslaite, älyrannekkeet, askelmittarit, vaaka, EKG (elektrokardiogrammi) -arvoja mittaavat laitteet, veren glukoosin mittauslaite ja spirometri. Edellä mainittujen mittauslaitteiden tulee mahdollistaa mittausarvon lähettämisen BT/BLE:lla vastaanottavaan mobiililaitteeseen. Insinöörityössä ei tulla luettelemaan tarkkaan verifioituja mittalaitteita valmistajakohtaisesti, sillä kyseiset verifioidut laitteet eivät kuulu julkisen tiedon piiriin.

3.3 Laitteen valinta- ja validointiprosessi

Mobiililaitteita valittaessa tulee olla valmis suunnitelma siitä, mitä tulee ottaa huomioon, jotta mobiililaite olisi täysin yhteensopiva DeviceHub-mobiilisovelluksen, tulevan MDM-ratkaisun ja haluttujen MDM-ratkaisuvaatimusten kanssa. Insinöörityössä pyritään painottumaan MDM-ratkaisun aihepiiriin, joten yksityiskohtaisempi laitetasoon keskittyminen jää vähemmäksi. Lyhyesti kerrottuna laitevalidointiprosessi käsittää monipuoliset testaukset sovellus- ja komponenttitasolla, jotta päästäisiin ihanteelliseen yhteensopivuustilanteeseen laitteita valittaessa.

3.4 MDM – Mobiililaitteiden hallinta

MDM on etähallintaohjelmisto, jonka avulla IT-osastot voivat toteuttaa käytäntöjä, jotka suojaavat, valvovat ja hallitsevat loppukäyttäjien mobiililaitteita. Tämä ei koske pelkästään älypuhelimia, vaan se käsittää myös tabletit, kannettavat tietokoneet ja jopa IoT (Internet of Things) -laitteet (10). Koska koronavirusepidemian vauhdittamana etätyö on yleistynyt ja siitä on tullut uusi normi. Mobiililaitteista on tämän seurauksena tullut erottamaton osa useimpia

organisaatioita. Näin ollen niistä on tullut tärkeä työkalu tuottavuuden ja tehokkuuden parantamiseksi. Tänä päivänä yritysten mobiililaitteet sisältävät yhä enemmän tärkeää yritystietoa, ja siksi ne voivat uhata tietoturvaa, jos ne hakkeroidaan, varastetaan tai kadotetaan. Siksi mobiililaitteiden hallinnasta on tullut entistäkin tärkeämpi osa-alue yritysten tietoturvan osalta. Modernin MDM-ratkaisun avulla IT- ja turvallisuusosastot voivat hallita kaikkia yrityksen ylläpitämiä laitteita niiden tyypistä tai käyttöjärjestelmästä riippumatta. Tämä auttaa pitämään kaikki yrityksen laitteet turvassa ja ylläpitämään työntekijöiden työtehokkuutta. (2.)

Esimerkkitapaus 1. Organisaatiossa on otettu käyttöön MDM-ratkaisu ja organisaation hallinnassa oleviin Android-mobiililaitteisiin on MDM-ratkaisussa asetetun käytännön mukaan pakotettu asentumaan yrityksen valmistama yksityinen mobiilisovellus. Kyseinen mobiilisovellus tukee vain Android 10 -käyttöjärjestelmäversiota. Organisaation Android-puhelimiin halutaan automaattisesti asentuvan käyttöjärjestelmän turvallisuusasetukset, mutta puhelimen käyttöjärjestelmää ei saa päivittää Android 11 -versioon. Kyseisessä esimerkkitapauksessa MDM-ratkaisun kautta on asetettuna laite- ja sovellustason käytäntö, joka MDM-ratkaisukohtaisesti tarkistaa kaikki siihen liitetyt laitteet, vastaako kyseisien laitteiden status niille asetettuja käytäntöjä.

Esimerkkitapaus 2. Mobiililaitteen loppukäyttäjä on jostain syystä poistanut käytäntövastaisesti laitteeseen asennetun mobiilisovelluksen. Tässä kohtaa laitekohtainen käytäntö havaitsee kyseisen laitteen statuksessa puutteen, ja se toteuttaa automaattisesti mobiilisovelluksen uudelleenasennuksen.

MDM-ratkaisun laitetason käytännöllä tarkoitetaan mobiililaitteen laite- ja käyttöjärjestelmäkohtaisten ominaisuuksien rajoittamista. Sovellustason käytännöillä taas tarkoitetaan mobiilisovellusten ominaisuuksien ja niissä liikkuvan tiedon rajoittamista MDM- ja mobiilisovelluksen tarjoamien ominaisuuksien puitteissa.

3.5 MTD – Mobiililaitteiden uhilta suojautuminen

Pääsääntöisesti MDM-ratkaisut sisältävät monipuolisia mobiililaitteiden turvallisuuteen keskitettyjä suojausominaisuuksia. Vastaan voi silti tulla tilanne, missä käyttöönotettu MDM-ratkaisun tarjoama laite-, sovellus- ja tietoturvaominaisuudet eivät ole riittäviä. Silloin tulee harkita lisäturvaa MTD (Mobile Threat Defense) -ratkaisusta, joka kykenee esimerkiksi suojaamaan mobiililaitteita laajoilta verkkohyökkäyksiltä. Tällä tarkoitetaan menetelmää tai ratkaisua, jolla on valmiudet mahdollistaa mobiililaitteiden, alustojen, sovellusten ja verkkojen suojaamisen useilta yleisiltä ja edistyneiltä uhilta. (11.)

Erilaiset MTD-ratkaisut käyttävät erilaisia tekniikoita. MTD-ratkaisut keräävät ja analysoivat mobiililaitteessa olevaa tietoa tunnistaakseen poikkeavaa käyttäytymistä ja torjuakseen uhkia. Tätä varten MTD-ratkaisut keräävät tietoa laitteista sekä lähteestä, josta tieto tulee laitteeseen. Tarkkailemalla laitteiden käyttäytymistä MTD-ratkaisut oppivat tunnistamaan haitallisen ja epäilyttävän käytöksen ja puuttumaan asiaan sen korjaamiseksi.

3.6 MAM – Mobiilisovellusten hallinta

Mobiilisovellusten hallinta (MAM, Mobile application management) on ohjelmistoratkaisujen joukko, joiden avulla järjestelmänvalvojat voivat ottaa käyttöön ja hallita turvallisesti mobiilisovelluksia yritys- ja henkilökohtaisissa mobiililaitteissa. Toisin kuin MDM, MAM-ratkaisu keskittyy sovellusten jakamiseen ja hallintaan valtuutetuille mobiililaitteilla. (12.)

Mobiilisovellusten hallinnan avulla järjestelmänvalvojat voivat soveltaa käytäntöjen toimintoja yksittäisiin sovelluksiin, jotka toimitetaan sitten esimerkiksi Google Play -sovelluskaupan kautta ja joita hallitaan laitehallintaympäristön kautta. (12.)

3.7 UEM – Yhdenmukaistettu päätelaitteiden hallinta

UEM:n (Unified Endpoint Management) tarkoituksena on yhdistää esimerkiksi MDM- ja MAM-palvelut saman ympäristön alle. Perinteiseen MDM-palveluun verrattuna UEM tarjoaa alustaa, jossa on yhdistettynä esimerkiksi MDM- ja MAM-palveluiden tarjoamien kokonaisuuksien lisäksi jopa etätyöpöytämahdollisuuksia. UEM:n tarkoituksena on mahdollistaa yhä useampien laitevalmistajien laitteiden ja eri käyttöjärjestelmien sisältävien laitteiden hallinta ja seurata yhdessä keskitetyssä ympäristössä. Tänä päivänä on tarjolla UEM-ratkaisuja, jotka tarjoavat laitehallintaa perinteisen MDM-ratkaisun lisäksi myös Linux- ja Chrome-alustan laitteille. (13.)

4 Insinöörityön tavoite ja lähtökohdat

4.1 Ongelma ratkottavaksi

Insinöörityön tavoitteena on fysiologisien mittauksien vastaanottavien mobiililaitteiden ja niihin asennettavien mobiilisovellusten hallinta ja seuranta etänä. Esimerkiksi voi tulla tilanne, jossa mittauslaite ja siihen BT/BLE-teknologialla yhdistetty mobiililaite ovat potilaan kotona, ja mittauksia vastaanottava mobiililaite menee DeviceHub-sovelluksen tai käyttöjärjestelmän virhetoiminnan johdosta sellaiseen virhetilaan, josta se ei pysty itsenäisesti toipumaan. Tässä tilanteessa potilas harvoin kykenee ohjeistuksista huolimatta saamaan mittauslaitekokoonpanoa toimimaan tavoitellusti, jossa mittaukset voisivat olla toteutettavissa normaalitilanteen mukaisesti. Vastaavia ongelmatilanteita ei ennen insinöörityön tuloksena löytynyttä MDM-ratkaisua saatu sen hetkisillä työkaluilla ja resursseilla ratkaistua ilman monimutkaisia ja kustannuksiltaan suuria järjestelyitä. Joissain asiakassopimuksissa oli hankittu alihankinnalla palvelu, joka toteutti kotikäynnin potilaan luona kartoittamassa tilannetta ja mahdollisuuksien mukaan korjasi ongelmatilanteen. Uudenmaan-läänin rajojen sisäpuolelle sijoitetut laitekokoonpanot, joissa oli todettu ongelmatilanteita, olivat tähän mennessä kerätty asiakasorganisaation tiloihin, joissa Medixinen edustaja kävi kartoittamassa ongelmatilanteen.

4.2 MDM-ratkaisujen kartoittaminen ja niille asetetut vaatimukset

Insinöörityön ensimmäisenä vaiheena on kartoittaa jo markkinoilla olevia MDM-ratkaisuja, jotka mahdollistavat Medixinen tarjoamien laitekokoonpanojen etähallinnan vaatimusten määrittämissä rajoissa. Erillisenä aihealueena projektissa otettiin tutkittavaksi mahdollisen henkilökohtaisen tiedon näkyvyys etähallintatilanteessa. Tässä on tarkoituksena se, että pyritään estämään mahdollinen tilanne, jossa MDM-ratkaisun ylläpitäjälle olisi nähtävillä terveystietoja.

Insinöörityötä varten on jo tiedossa vaatimukset, joita MDM-ratkaisun tulee mahdollistaa. Näitä vaatimuksia ovat mobiilisovellusten asentaminen ja päivittäminen, mobiililaitteen hallinnointi ja Kiosk Moden käyttöönoton mobiililaitteessa. Luvussa 5 (Vaatimukset MDM-ratkaisulta) käydään tarkemmin läpi mitä Kiosk Modella tarkoitetaan.

4.3 MDM-ratkaisun käyttöönoton hyödyt

MDM-ratkaisun päätarkoituksena on antaa yrityksille mahdollisuus keskittyä työntekijöidensä tuottavuuden parantamiseen antamalla heidän käyttää yrityksen tietoja yrityksen tai henkilökohtaisesti omistettujen mobiililaitteiden avulla. MDM-ratkaisut voivat auttaa saavuttamaan tämän saumattomasti ja yksinkertaisesti. (14.)

MDM:n tarkoituksena on pitää yritystiedot suojattuna ja varmistaa, että yritykset hallitsevat luottamuksellisia tietojaan. Jos mobiililaite katoaa tai varastetaan, MDM voi lukita ja pyyhkiä kaikki tiedot etänä. Etälukitus- ja pyyhintäominaisuuksien avulla yritykset voivat pitää laitteet ja tiedot turvassa. (14.)

MDM:n avulla yritykset kykenevät hallitsemaan käytäntöjä ja lisätoimintoja keskitetysti. MDM-ratkaisulla voidaan estää vaarallisia verkkosivustoja ja

materiaaleja työntekijöiltä. Tämä suojaa yritystietoja ja sovelluksia haittaohjelmilta ja tietomurroilta. (14.)

Eristettävyys on tärkeä ominaisuus yritystietojen turvaamisessa liikkuvalle työvoimalle. Tämä tunnetaan myös nimellä Kiosk Mode. Laitehallinnan yhteydessä yritystiedot ja sovellukset erotetaan laitteenhaltijasta. Tällä estetään mobiilipohjaisia hyökkäyksiä (kuten tekstin tai sovellusten kautta), riskialtista käyttäjän toimintaa ja jopa yksinkertaisia onnettomuuksia vuorovaikutuksessa tiettyjen sovellusten kanssa, joissa on arkaluonteisia yritystietoja.

5 Vaatimukset MDM-ratkaisulle

5.1 Huomioitavaa MDM-ratkaisun valintaa tehtäessä

MDM-ratkaisua ei voida valita mielivaltaisesti, sillä tarjontaa ja ominaisuuksien monipuolisuutta löytyy markkinoilta laajalti. Ennen ratkaisun valintaa tulee ottaa huomioon muutamia seikkoja, miksi yritys tarvitsee MDM-ratkaisua ja mitä siltä vaaditaan. Seuraavaksi listataan ominaisuuksia, joita pitkän pohdinnan päätöksenä on valittu vaadittaviksi ratkaisulta.

Yhtenä ratkaisevimmista Medixinen asettamista vaatimuksista MDM-ratkaisulta on mahdollistaa Kiosk Moden käyttöönotto mobiililaitteissa. Kiosk Modella tarkoitetaan käytännössä sitä, että laite on lukittu tilaan, tai niin sanottuun erilliseen istuntoon, jossa laite- ja/tai sovelluskohtainen käyttö on rajoitettu hyvin minimalistisiin mahdollisuuksiin. Esimerkkinä on tilanne, missä loppukäyttäjällä on mahdollistettu säätää laitteen asetusten osalta vain ääni- ja BT/BLE-laitteiden liittämisenasetuksia. Kiosk Modessa voi myös esimerkiksi asettaa loppukäyttäjälle käytettäväksi vain yksi tai kaksi mobiilisovellusta. Medixinen tapauksessa Kiosk Modella voisi mahdollistaa sen, ettei loppukäyttäjä voisi saada mobiililaitetta asetusten puolesta tilaan, missä mobiililaite ei kykenisi lähettämään mittaustuloksia verkko teitse Medixine Suite -palveluun, tai voisi vahingossa poistaa Medixine DeviceHub -mobiilisovelluksen. DeviceHub-sovelluksen vahingossa poistaminen aiheuttaisi todella suuren

ongelmatilanteen, jos esimerkiksi potilaan sijainti olisi sellainen, mihin Medixinen edustaja ei kykenisi pääsemään paikan päälle.

Toisena tärkeänä vaatimuksena on mahdollistaa mobiililaitteeseen asennetun yksityisen sovelluksen päivitys etänä. Yksityisellä sovelluksella tarkoitetaan tässä tapauksessa Medixinen toteuttamaa DeviceHub-mobiilisovellusta, joka on ladattuna Google Play Storen Private -sovelluskauppaan, ei esim. Google Play Storen Public-sovelluskauppaan, jossa kaikki sinne julkaistut mobiilisovellukset ovat julkisesti ladattavissa.

5.2 Tuettavat laitteet

Projektin aikana tulee ottaa huomioon, etteivät MDM-sovellukset oletuksena tue kaikkia laitevalmistajien laitteita ja käyttöjärjestelmiä. Joten on tärkeää suunnitella ja toteuttaa testit etukäteen eri käyttöjärjestelmien omaavilla ja eri valmistajien tarjoamilla laitteilla. Laitetestaamista tulee käyttää vaatimuksena, mitä laitteita MDM-ratkaisun tarvitsee tukea. Tämän hetkisenä käyttöjärjestelmäkohtaisena vaatimuksena on kyetä hallitsemaan Android-käyttöjärjestelmän sisältäviä matkapuhelimia. Tässä vaiheessa on myös jo tiedossa, että DeviceHub-etämittausratkaisua ei tulla toteuttamaan Applen iOS-mobiilialustalle, sillä Applen mobiililaitteiden hinnan ja lopullisen hyötysuhteen takia tämä ei vain olisi kannattavaa. Medixinellä on lähiaikoina otettu puheeksi myös mahdollinen firman sisäisten mobiililaitteiden hallinta ja seuranta, joten MDM-ratkaisu voisi kattaa matkapuhelintuen lisäksi myös Apple- ja Windows-käyttöjärjestelmän omaavat tietokonelaitteet.

5.3 Turvallisuuden hallinta

Yhtenä tärkeänä aiheena on mobiililaitteiden turvallisuuden hallinta. Laitteiden osalta, jotka ovat etähallinnan piirissä, tulee ottaa huomioon se, että laitteen ja web-palvelun välillä liikkuva tieto pysyy turvassa. Tulee myös ottaa huomioon toivottava kyky laaja-alaisempaan laitehallintaan, eli hallita mahdollinen tiedon poisto, mobiililaitteen lukitseminen, tiedon tyhjentäminen ja ääritilanteessa myös

laitteen tehdasasetuksille asettaminen esimerkiksi laitevarkaustilanteessa. (15, s. 2.) Ennen muuta on tärkeää ottaa selvää, mitä MDM-ratkaisu tarjoaa turvallisuuden hallinnan osalta, jotta ihannetilanteessa ominaisuuksiensa puolesta se mahdollistaa siihen liitettyjen laitteiden turvallisuuden hallinnan.

5.4 Koeaika

Miltei jokainen MDM-ratkaisupalveluntarjoaja on valmis tarjoamaan ennen virallista käyttöönottoa koeajan, jonka aikana organisaatio voi ottaa ratkaisun käyttöön ja rekisteröidä laitteensa palveluun ja ajaa kaikki mahdolliset testit. Tämä on mahdollistanut organisaatiolle saada paras mahdollinen kuva siitä, pystyykö mobiililaitteiden hallintaratkaisu vastaamaan organisaation asettamiin vaatimuksiin. Insinöörityön osalta on jo todettu, että useat palveluntarjoajat ovat valmiita pidentämään koeaikaa, jos sille olisi tarvetta. Koeajan pidennys on helpottanut paljon tilannetta, koska insinöörityö on pyritty toteuttamaan muun normaalin työn ohessa ja insinöörityöhön käytettävä aika on ollut jatkuvasti tiukilla.

5.5 Kustannus

Tuotekustannukset ovat yksi suurimmista ratkaisevista tekijöistä, kun käydään läpi projektin aikana tutkittavia MDM-ratkaisuvaihtoehtoja. Medixine ei ole määrittänyt tarkkaa budjettia hankittavan ratkaisun osalta. Etämonitorointi on kuitenkin hintakilpailtu liiketoiminta-alue ja senttienkin heitot kuukausittaisessa veloituksessa muodostuvat merkittäväksi kustannukseksi volyymin kasvaessa. Miltei jokainen MDM-palvelun tarjoaja laskuttaa ratkaisun käytön käytössä olevien liitettyjen laitteiden määrän mukaisesti. Tarjolla olevien MDM-ratkaisujen osalta ei ole suuria hintaeroja yhtä laitetta kohden. Laitemääräkohtaisesta laskutusmenetelmästä suuresti poiketen, yhtenä testattavana MDM-ratkaisuna Microsoft Intunen käyttöönottokustannukset perustuvat palvelun ylläpitäjäkohtaiseen lisenssien määrään, ei-liitettyjen laitteiden määrään.

5.6 Sovellusten hallinta

Hallittaviin mobiililaitteisiin on tarve asentaa tiettyjä yrityssovelluksia tai kolmannen osapuolen sovelluksia. Siksi on selvitettävä, onko sovellusten hallinta osa mobiililaitteiden hallintaratkaisua ja miten sovellus- tai käyttöjärjestelmäpäivitykset jaetaan palveluun liitetyille laitteille tai laiteryhmille. Sovellusten hallintaan tulee kohdistumaan paljon painetta projektin osalta, sillä tämänhetkisestä tilanteesta johtuen DeviceHub-sovelluksen päivittäminen vaatisi päästä potilaan luokse paikan päälle toteuttamaan sovelluksen päivitys. Edellä mainitusta johtuen suurimpana vaatimuksena MDM-sovellukselta on mahdollisuus Medixine DeviceHub-sovelluksen asentaminen ja päivittäminen etänä.

5.7 Laitteiden valvonta ja seuranta

Mobiililaitteiden valvonta ja seuranta on yksi tärkeimmistä MDM-ominaisuuksista, jotka mahdollistavat laitteiden laaja-alaisen valvonnan jopa automatisoiduilla toiminnallisuuksilla. MDM-ratkaisua valittaessa on tärkeää huomioida, tarjoaako tuleva ratkaisu sijainninseuranta- ja maantieteellistämisominaisuuksia vai ei, mahdollistaako ratkaisu Kiosk Moden käyttöönoton ja siinä yksittäisen sovellustilan vai usean samanaikaisen sovelluksen tilan sekä useita muita ominaisuuksia liittyen laitevalvontaan ja laitteen käytön rajoittamiseen. Laiteseurannan automatisoinnilla voidaan toteuttaa automatisoituja toimintoja, jotka ilmoittavat laiteylläpitäjälle, jos laitteen turvallisuuspäivitykset eivät ole ajan tasalla. Useassa MDM-ratkaisussa on myös toteutettu laitekohtaista tiedon seurantaa, joka mahdollistaa erinäisten hälytysten asettamista, joilla voidaan valvoa yksityiskohtaisesti laitteen sisältämää tietoa.

5.8 Sisällön hallinta

Yrityksen ja laitteenhaltijan tiedon turvallisuus on yksi liiketoiminnan tärkeimmistä prioriteeteistä. Hyvän MDM-ratkaisun avulla organisaatio voi

ladata, jakaa ja muokata sisältöä hallintapaneelin kautta MDM-ratkaisuun liitetyille laitteille. Medixinen tarjoamissa mobiililaitteissa, joiden on määrä vastaanottaa vain fysiologisia mittausarvoja, ei pääsääntöisesti tule sisältämään Medixinelle tai asiakasorganisaatioille arkaluontoista tietoa. Laitteiden sisältämän tiedon turvaaminen tullaan toteuttamaan hallitulla laitekohtaisella seurannalla ja tarkoin suunnitelluilla käytäntöasetusten käyttöönotolla.

5.9 Mobiililaitteiden suojauksen hallinta

Kun organisaatiolla on tiedossa, mitkä laitteet tullaan ottamaan käyttöön MDM-ratkaisun kanssa, tulee aika arvioida ympäristölle aiheutuva turvallisuusriski, joka on yksi yleisimmistä puutteista perinteisissä MDM-ratkaisuissa. Kuvitellaan, että käytössä on tietoturvaratkaisu, joka voisi antaa informaatiota kaikkien laitteiden tietoturvatilasta, esimerkiksi käyttääkö laite salasanoja, mikä käyttöjärjestelmä- ja selainversio on laitteeseen asennettuna ja ovatko ne ajan tasalla. Jos jokin edellä mainituista käy toteen, olisi laitteiden suojauksen tilaan perustuen suositeltavaa olla mahdollista rajoittaa laitteen käyttöä, suojauksen tilan seurantaa ja mahdollisuus havaita ja pysäyttää vanhentuneiden ja haavoittuvaisten laitteiden käyttämistä (16, s. 5). Yhtenä helpoimpana ja yleisimpänä mobiililaitteiden suojaustapana on pakottaa mobiililaitteisiin automaattisesti asentuvan virustentorjuntaohjelmiston. Kyseistä virustentorjuntaohjelmistoa kohtaan voisi esimerkiksi asettaa käytäntöasetuksen, joka estäisi kyseisen ohjelmiston poistamisen mobiililaitteelta.

5.10 Käytäntöjen täytäntöönpano ja vaatimustenmukaisuus

Organisaatioiden, jotka suunnittelevat MDM-ratkaisun käyttöönottamista hallitakseen mobiililaitteita, on oltava valmiita noudattamaan tietoturvakäytäntöjä vähentääkseen tietoturvaloukkausten riskejä ja estääkseen haavoittuvia tai suojaamattomia laitteita pääsemästä arkaluonteisiin tietoihin. Suojauskäytännöt ovat yksilöllisiä ja siksi pitäisi pystyä mukauttamaan tietoturvakäytäntöjä esimerkiksi tiettyihin sovelluksiin liittyvistä riskeistä.

Esimerkiksi suojaukseen liittyvä käytäntöasetus estää mobiililaitteelle asennetun arkaluontoista tietoa sisältävän sovelluksen käytön, jos suojausasetuksen vaatimat päivitykset eivät ole mobiililaitteeseen asennettuna. Mobiililaitteella on silti mahdollista käyttää muita asennettuja sovelluksia, jotka eivät sisällä arkaluontoista tietoa. (16, s. 5.)

Organisaation tulisi harkita MDM-ratkaisua, joka painottaa ottamaan käyttöön turvallisuuskäytäntöjä sen sijaan, että antaisi laitteen haltijan käyttää laitetta vapaasti. Näin voidaan asettaa johdonmukaisia suojauskäytäntöjä, joka mahdollistaa saumattoman käyttäjäkokemuksen.

6 MDM-ehdokkaat

6.1 MDM-sovellus ehdokkaiden vertailu

Alustavana suunnitelmana oli valita laajasta markkinatarjonnasta kolme potentiaalisinta MDM-palveluntarjoajan tuotetta tarkempaan seulontaan. Näitä testaamalla saataisiin selvitettyä, mikä vaihtoehdoista täyttäisi parhaiten Medixinen asettamat vaatimukset ja mitkä palvelun ominaisuudet olisivat painoarvoltaan ratkaisevimmat lopullisen valinnan tekemisessä. Ajanpuutteesta ja tarjonnan laajuudesta johtuen kolmen vertailuun otettavan sijasta projektissa päädyttiin valitsemaan testattavien listalle vain kaksi potentiaalisinta tuotetta. Tällä hetkellä Medixinellä ei ole käytössä kuin Android-käyttöjärjestelmän omaavia ja Motorola-laitevalmistajan tarjoamia matkapuhelimia, joten insinöörityö keskittyy edellä mainittujen laitteiden käyttöönottoon MDM-ratkaisussa. MDM-sovellusehdokkaiden osalta laitteiden liitettävyysmahdollisuuksista riippuen on otettava huomioon muut mobiililaitevaihtoehdot, kuten tabletit ja kannettavat tietokoneet, vaikka nämä laitteet eivät kuulukaan insinöörityön aihepiiriin.

MDM-ratkaisujen vertailuun valittiin Microsoftin Intune ja Sophos Mobile. Microsoft Intune valittiin kandidaatiksi niillä perustein, että tiedettiin jo entuudestaan Microsoft Intunen kuuluvan osaksi Microsoft Azuren

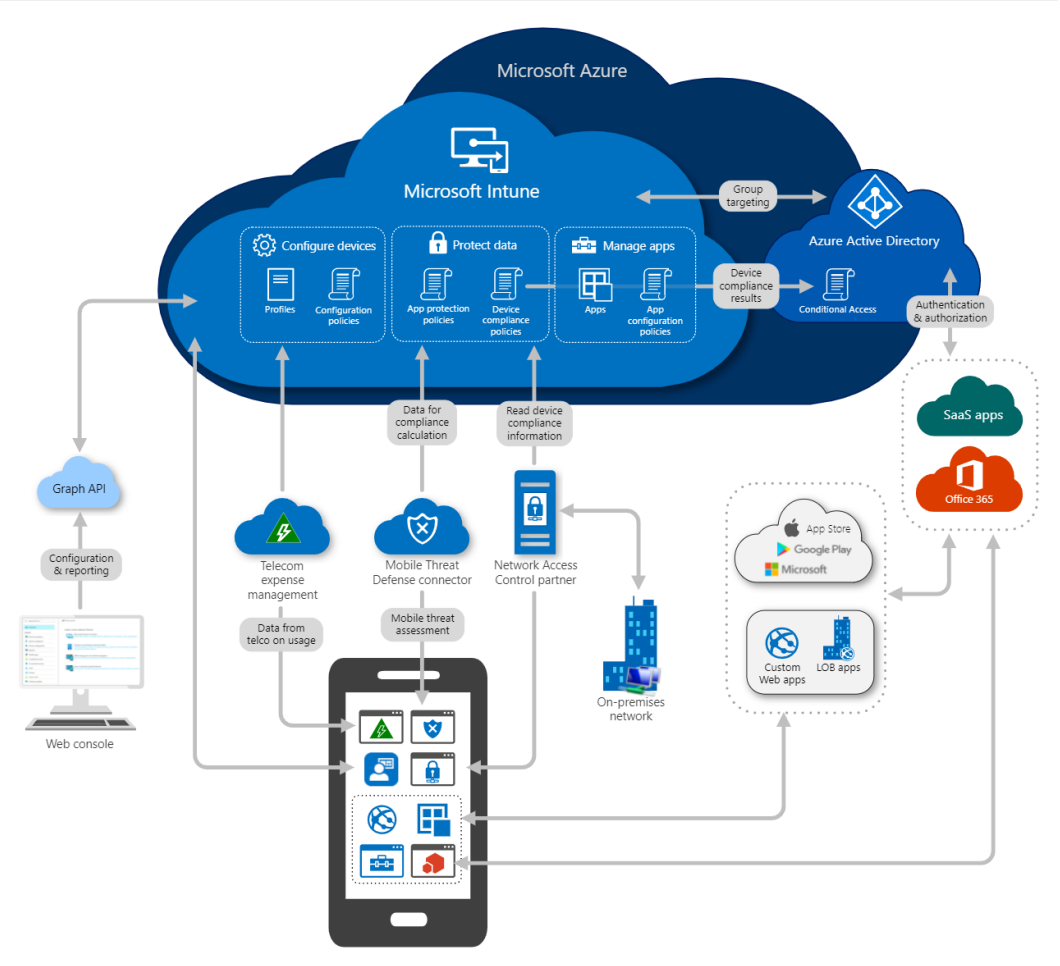
pilvipalvelukokonaisuutta. Tästä syystä se oli helposti lähestyttävissä ja valmiiksi jo osa Medixinen käytössä olevaa Azure-pilvipalvelua, johon ei vain ollut vielä ehditty tutustumaan. Toiseksi kandidaatiksi valittiin Sophos Mobile. Kyseinen kandidaatti oli ollut Medixinellä testauksen alla muutama vuosi aiemmin sen aikaisen järjestelmäasiantuntijan koekäytössä. Tästä syystä kyseisestä ratkaisusta oli Medixinellä jo ennakkotietoa ja -kokemusta.

Internethaun perusteella mahdollisten MDM-ratkaisujen osalta tuli nopeasti ilmi, että tämän hetken suosituin MDM-ratkaisu näytti olevan Miradoren toteuttama. Miradoren MDM-ratkaisu sai selvästi arvostusta monipuolisten ominaisuuksien ja tarjolla olevan ilmaisversion takia, jota yksikään muu palveluntarjoaja ei ole tällä hetkellä vielä valmis tarjoamaan. Vaikka moni muukin MDM-ratkaisuvaihtoehto vaikutti olevan hyvä kandidaatti otettavaksi mukaan projektiin edellisessä luvussa jo mainittujen syiden takia jätettiin lähinnä ajanpuutteen vuoksi kandidaattilistalle vain Microsoftin Intune ja Sophos Mobile.

6.2 Microsoft Intune

6.2.1 Yleistä Microsoft Intunesta

Intune on pilvipalveluun pohjautuva UEM-palvelukokonaisuus, joka keskittyy mobiililaitteiden ja mobiilisovellusten etähallintaan ja -seurantaan (MDM ja MAM). Se on osa Azuren suurta pilvipalveluympäristöä. Intune on Microsoftin näkemys siitä, miten toteuttaa monipuoliselle MDM-palvelumarkkinoille ratkaisu, joka yhdistettynä Azuren muihin palveluihin ja Microsoft Office365:een luo kokonaisuutena ympäristön, jossa laitehallinnalle ja -seurannalle ei löydy ominaisuuksien puolesta miltei lainkaan puutteita. Intunea voidaan hallita Azure- kuin myös Office365-portaalin kautta. (17.) Kuvassa 3 on esitetty Microsoft Intunen arkkitehtuuri, joka tarjoaa monipuoliset mahdollisuudet laite- ja sovellushallinnalle sekä seurannalle. (18.)



Kuva 3. Microsoft Intunen arkkitehtuuri.

Microsoft Intune tukee kaikkia yleisimpiä mobiililaitteita valmistajasta ja käyttöjärjestelmästä riippumatta. Intune on osa Microsoftin Enterprise Mobility + Security -palvelupakettia ja sen yksi suurimpia etuja on sen integraatio Azure AD:n (Active Directory) kanssa. Tämä mahdollistaa organisaatioiden hallita Intuneen liitettyjä laitteita jopa yrityksen omalle palvelimelle asennetusta AD:sta käsin, kunhan organisaatio on mahdollistanut Azure AD:n ja organisaation oman paikallisen AD:n integraation Azuressa. (17.)

Intunen ensimmäinen versio julkaistiin markkinoille vuonna 2011, ja siitä tuli osa Azuren pilvipalvelukokonaisuutta vasta vuonna 2016. Tuolloin se tunnettiin vielä nimellä Microsoft Endpoint Manager. Vuonna 2021 Microsoft kehittää jatkuvasti Intunen ominaisuuksia ja Microsoft on perustanut palvelulle oman osionsa Microsoftin Customer community -sivustolle, jossa palvelua käyttävät

organisaatiot voivat julkaista toiveitaan ja ideoitaan Intunen kehitykseen liittyen ja ilmoittaa myös mahdollisista virhetilanteista. (19.)

6.2.2 MAM Intunessa

Microsoft Intunen UEM-kokonaisuuteen sisältyy MAM-ominaisuus, joka mahdollistaa monipuolisen mobiilisovellusten hallinnan ja seurannan. Intunen MAM-ominaisuus on suunniteltu suojaamaan organisaatioiden tietoa laite- kuin myös mobiilisovellustasolla, mukaan lukien yksityiset ja Google Play Store-sovellukset. Intunessa on mahdollista hallita sovellustason tietoa niin, että vain yritykseen liittyvää tietoa käsitellään. (20.)

6.2.3 Intunen ominaisuuksien kartoittaminen ja käyttökokemus

Microsoft Intune on MDM-sovellusvaihtoehdoista lähtökohtaisesti potentiaalisin vaihtoehto. Medixine käyttää pilvialustanaan Microsoftin Azure-pilviympäristöä ja Medixinellä on Microsoft Partners sopimus, joka sisältää Enterprise Mobility + Security E3 IUR -tuotepaketin, johon taas sisältyy yhtenä palveluna Microsoft Intune -lisenssi (21). Tämä tarkoittaa käytännössä sitä, että Microsoft Intune ei MDM-ratkaisuvaihtoehtona tulisi maksamaan yritykselle lainkaan ylimääräistä verraten kaikkiin muihin MDM-vaihtoehtoihin. Edellä mainitusta syystä Intunen osalta ei ole koeaikaa, joten Medixine pääsee koekäyttämään palvelua saman tien kaikkine ominaisuuksineen.

Yhtenä suurena etuna Microsoft Intunelle on olla osana Microsoftin laajaa ohjelmistorepertuaaria ja miltei kaikki Microsoftin tarjoamat palvelut on mahdollista yhdistää toisiinsa integraatioilla ja API (Application Programming Interface) -kutsuilla. Tästä syystä Intuneen liitetyt laitteet näkyvät myös Azure AD:ssa, jota Medixine käyttää laite- ja käyttäjähallintatyökalunaan. Azure AD mahdollistaa sen, että Intuneen liitettyjä laitteita kyetään hallitsemaan ja seuraamaan Azuren osalta osana yrityksen infrastruktuuria. Intuneen liitettyjen laitteiden seurantaan käytettäviä toimintoja kyetään Azuren resurssienhallinnan ansiosta eristämään omiin resurssiryhmiinsä, joten laitteiden sisältävää tietoa

seuraavat toiminnot ovat turvallisesti eristettynä kaikesta muusta Azuressa olevista yrityksen resursseista. (22.)

Yhtenä suurena plussana on, että Intuneen liitettävät laitteet voidaan eristää omiin laiteryhmiinsä, joissa ei ole lainkaan lisättävien laitteiden määrärajoitusta. Tämä mahdollistaa sen, että Intunessa voidaan asettaa asiakasorganisaatiokohtaiset laitteet omiin asiakaskohtaisesti nimettyihin ryhmiin ja ryhmille voidaan asettaa käyttöön asiakasorganisaation ja Medixinen vaatimat käytäntösäännöt.

Microsoft Intunea käyttäville yrityksille on tarjolla niin sanottu ZERO-TRUST-malli, jota on hyvä käyttää pohjana käytäntöjä suunnitellessa (23, s. 1-2). Se on Microsoftin tarjoama ohjeistusdokumentaatio siitä, miten yritykset, jotka ovat ottamassa Intunea käyttöönsä, voisivat varmistaa heti käyttöönoton alussa sen, että Intuneen liitetyt laitteet ja yrityksen tieto olisivat suojattuja. ZERO-TRUST-mallilla tarkoitetaan käytäntöjen asetusmallia, jossa lähtökohtaisena ajatuksena on luoda käytäntöasetuskokonaisuus, joka estää mobiililaitteessa kaiken ylimääräisen toiminnallisuuden ja käyttäjältä vaaditaan aina vähintään kaksivaiheista tunnistautumista kirjautuessaan palveluihin. (23.)

Ei plussaa, jos ei miinustakin. Microsoft Intune niin monipuolisena ja potentiaalisena vaihtoehtona kuin onkin, myös sisältää muutamia huonoja ominaisuuksia. Esimerkkinä on Intunen monimutkainen GUI, joka on helposti omaksuttavissa, jos muuten on tottunut käyttämään Azuren tarjoamia palveluja, mutta ensikertalaiselle GUI voi aiheuttaa paljon harmaita hiuksia sen käyttöä opeteltaessa. Toisena miinuspuolena on Microsoft Intunen dokumentaatio. Se on toteutettu perinteisellä Microsoftin tavalla, josta syystä Intunen tarjoamista ominaisuuksista on vaikeahko heti löytää mainintaa muutenkin laajasta Microsoftin dokumentaatioarsenaalista.

6.2.4 Microsoft Intunen käyttöönottoprosessi

Android-mobiililaitteen liittäminen Microsoft Intune -sovellukseen voidaan toteuttaa palauttamalla puhelin tehdasasetuksille ja sen jälkeen Microsoftin tarjoamien ohjeiden mukaisesti toteuttaa Android-mobiililaitteen ja Intunen välinen yhteys. Toisena vaihtoehtona on jo käytössä olevalla puhelimella Google-tiliin kirjautuminen Google Storeen ja Intune Company Portal App:n lataaminen ja tämän avulla laitteen liittäminen Intune-sovellukseen. (24.)

Käyttöönotossa mobiililaitteet liitettiin palveluun palauttamalla puhelimet tehdasasetuksille ja sen jälkeen toteuttamalla liitos QR-koodin (Ruutukoodi) lukemisprosessilla (25). Kun mobiililaitteen ja MDM-sovelluksen liitos oli saatu toteutettua, tuli palveluun luoda ryhmä, johon jo liitetyt mobiililaitteet lisättiin. Perustetulle ryhmälle asetettiin turvallisuuskäytäntöjä ja monia muita käyttöä helpottavia tai rajoittavia käytäntöjä. Nämä käytännöt tulivat voimaan ryhmiin lisätyille laitteille.

Testien ohessa oli todettavissa, että ryhmät ja niihin käyttöön otettavat käytännöt on hyvä suunnitella jo etukäteen, ennen kuin ryhmiin lisättävät laitteet liitetään MDM-palveluun. Jälkikäteen lisättyjen käytäntömuutosten siirtyminen mobiililaitteille vaikutti kestävän ajoittain yllättävänkin pitkään. Yleisimmin uuden asetuksen voimaan tuleminen jo liitetylle laitteelle kesti noin.5 minuuttia, mutta joskus käytäntömuutosten voimaan tuleminen laitteelle saattoi kestää jopa 30 minuuttia. Microsoftin dokumentaatioon perustuen Intunessa on omat määritykset sille, miten se toteuttaa käytäntö-asetusten synkronointi-intervalleja liitettyjä laitteita kohtaan (26). Microsoftin dokumentaation perusteella synkronointi-intervallivälit pitenevät perustuen siihen, kuinka pitkään laite on ollut palveluun liitettynä. Synkronointi-intervallivälit ovat eri pituisia riippuen siitä, mikä käyttöjärjestelmä laitteessa on asennettuna. Android-käyttöjärjestelmän sisältävää laitetta kohtaan synkronointi-intervallivälit ovat palveluun juuri lisättyä laitetta kohtaan seuraavanlaiset: 3 minuutin välein 15 minuutin ajan, 15 minuutin välein 2 tunnin ajan, siitä eteenpäin joka 8 tunnin välein. Nämä samat intervallivälit pätevät myös, jos laitteeseen kohdistettuun käytäntöasetukseen

tehdään jokin muutos. Jos jostain syystä palvelu ei saa laitteeseen yhteyttä, käytäntöasetuksessa tehdyn muutoksen voimaan tuleminen laitteessa voi viivästyä pidemmäksikin aikaa. Edellä mainittuun perustuen testeissä koettu käytäntöasetusten voimaan tulemisen viive saattoi juurikin johtua siitä, että palvelun ja laitteen välisessä yhteydessä on juuri sillä hetkellä ollut jokin katkos. Synkronointi on myös toteutettavissa manuaalisesti. Intunen portaalissa tulee paikantaa kyseinen laite tai laiteryhmä. Laiteryhmän näkymästä löytyy oma painikkeensa manuaalisen synkronoinnin toteuttamiselle. Samainen painike löytyy mobiililaitteessa löytyvässä Intune-sovelluksen asetukset-osiossa. (26.)

6.3 Sophos Mobile

6.3.1 Yleistä Sophos Mobilesta

Sophos Mobile on yrityskäyttöön suunniteltu web-pohjainen mobiililaitteiden hallinta- ja seurantaratkaisu. Se on osa Sophoksen pilvialustaa, jonka palveluihin Sophos Mobilen lisäksi kuuluu useita yritysten käyttöön tarkoitettuja tieto- ja laiteturvallisuuteen liittyviä palveluratkaisuja (27 Sophos Mobile. 2021. Sophos Mobile user documentation). Sophos Mobile on pilviympäristössä olevan palvelun sijasta mahdollista myös asentaa on-premise yrityksen omalle palvelimelle. Sophos Mobilen ensimmäinen versio julkaistiin 28. huhtikuuta vuonna 2011. Tuolloin se tunnettiin vielä nimellä Sophos Mobile Control. (28.)

6.3.2 Sophos Mobilen ominaisuuksien kartoitus ja käyttökokemus

Sophos Mobile on vaihtoehdoista teknisten ominaisuuksien ja GUI:n yksinkertaisuuden ja loogisuuden puolesta potentiaalisin. Se on helposti lähestyttävä vaihtoehto, jonka käyttöönotto mobiililaitteessa on toteutettu kilpailijaansa verraten yksinkertaisemmin. Tämä tarkoittaa sitä, että loppukäyttäjällä sijaitsevaan laitteeseen on ladattavissa erillinen sovellus, joka mahdollistaa palvelun käyttöönoton ilman ylimääräistä tehdasasetuksille palauttamista, jota taas miltei jokainen muu MDM-kilpailija vaatii liitettävältä laitteelta. Tämä mahdollistaa mobiililaitteen liittämisen MDM-palveluun, vaikka

laite olisi fyysisesti organisaation tavoittamattomissa, kunhan mobiililaite on yhdistettynä internetiin. Jokainen MDM-ratkaisu tarjoaa koeajan tutustua palveluun, joka on Sophos Mobilen osalta 30 päivää. (29.)

Sophos Mobilea tarjotaan alustavasti kolmena erinäisenä lisenssipakettina, jotka organisaatiot voi vapaasti valita käyttöönsä. Jos ensin valitussa paketissa eivät ominaisuudet riitä, voi organisaatio päivittää lisenssipakettiaan laajempaan tarjontaan (30, s. 4). Taulukossa 2 on lueteltu tarjolla olevat lisenssipaketit. (30, s. 4.)

Taulukko 2. Sophos Mobilen tarjolla olevat lisenssipaketit ominaisuuksineen.

Sophos Mobile

Licensing Overview

	Sophos Mobile Advanced	Sophos Mobile Standard	Intercept X for Mobile
Device Management	✓	✓	-
Application Management	✓	✓	-
Content Management	✓	-	-
Sophos Container (Secure Email, Secure Workspace)	✓	-	-
Malware, ransomware, PUA, spam protection	✓	-	✓
Web protection against malicious online content	✓	-	✓
MitM (man-in-the-middle) detection	✓	-	✓

Ominaisuuksiltaan lisenssipaketti Sophos Mobile Standard vastaa jo miltei täydellisesti Medixinen asettamia vaatimuksia muutamaa pientä seikkaa lukuun ottamatta. Sophos Mobilessa on muutamat asiat, joiden takia se ei ole täydellinen valinta Medixinellä käyttöönotettavaksi MDM-ratkaisuksi. Esimerkiksi testikäyttöönotossa tuli ilmi, että yhteen laiteryhmään voi parhaimmillaan liittää vain 15 laitetta kerrallaan. Tämä aiheuttaa sen, että jos palveluun on liitettynä esimerkiksi tuhat mobiililaitetta, viisisataa toiselle asiakkaalle kohdistettuna ja toiset viisisataa toiselle asiakkaalle kohdistettuna ja samainen käytäntösääntö halutaan jokaiseen näihin laitteisiin asetettavan aiheuttaa ongelmatilanteen. Tässä ongelmatilanteessa tulee tehtäväksi ylimääräisiä hiirenpainalluksia palvelun päässä eikä laiteryhmiä saada yksinkertaistettua niin, että olisi yksi

laiteryhmä asiakasyrityksen nimellä ja toinen toisen asiakasyrityksen nimellä ja molemmille laiteryhmille saataisiin helposti kohdistettua omat käytäntösäännöt.

Toinen iso miinus Sophos Mobilessa on sen kustannus. Sophos Mobilen käyttö tulisi kustantamaan Medixinelle jo annetun tarjouksen mukaan 1,5 €/mobiililaite/kk. Esimerkkinä, jos palveluun olisi liitettynä suurelle asiakasorganisaatiolle kohdistetut 10 000 mobiililaitetta, loppusummaksi tulisi niinkin suuri summa kuin 15 000 €/kk. Medixinen periaatteena on laskuttaa MDM-ratkaisunkäyttö asiakasorganisaatiolta. Medixine on tässä vaiheessa jo saanut osviittaa siitä, etteivät asiakkaat ole alustavasti valmiita kustantamaan vastaavia kuluja MDM-ratkaisun käyttöönotolta.

6.3.3 Sophos Mobilen käyttöönottoprosessi

Sophos Mobilen MDM-ratkaisun käyttöönotto Android-mobiililaitteella voidaan toteuttaa mobiililaitteen palauttamisella tehdasasetuksille ja tämän jälkeen ohjeiden mukaan toteuttaa liitos Sophos Mobile -sovellukseen. Android-mobiililaitteen ja Sophos Mobile -sovelluksen välinen liitos toteutetaan lukemalla mobiililaitteella MDM-sovelluksessa generoitu QR-koodi tai QR-koodin käsin kirjoittamisella liitosprosessin aikana. Vaihtoehtoisena liitostapana on Google-palveluun kirjautuminen jo käytössä olevalla puhelimella. Tämä vaatii käyttäjältä aktiivisena olevat Google-tunnukset. Google Play Storesta on ladattava Sophos Mobile enrollment app, jonka avulla Sophos Mobile MDM -sovellukseen liittäminen saadaan toteutettua (29). Sophos Mobilen osalta 30 päivän koekäyttöaika ei riittänyt omaksumaan riittävästi Sophos Mobilen tarjoamia ominaisuuksia, joten lisäaika koekäytölle oli tarpeen, jonka myös Sophos Mobilen yhteyshenkilö Medixinen testikäytölle salli.

7 Johtopäätökset

Mobiililaitteiden käyttö yritysten työvälineinä on yleistynyt räjähdysmäisesti viimeisen kymmenen vuoden sisällä ja niiden sisältämä tieto lisääntynyt. Nyt jos koskaan on aika miettiä, miten yritysten työntekijät käyttävät yrityksen tietoa

mobiililaitteissaan ja miten yrityksen työntekijöiden mobiililaitteita saataisiin hallittavaksi esimerkiksi yksinkertaisen ongelmatilanteen sattuessa, oli laite sitten työntekijän tai yrityksen omistama laite. Olisi aika myös miettiä, miten mobiililaitteiden ja niissä olevan tiedon seuranta ja hallinta kyetään toteuttamaan MDM-ratkaisun käyttöönotolla. MDM-ratkaisut ovat yleistyneet ja on miltei suositeltavaa, että jokaisen yrityksen tietoa käyttävät laitteet ovat jollain tapaa hallittavissa tai vähintään kyetä seuraamaan, miten ja missä laitteissa yrityksen tietoa käytetään. MDM-ratkaisun käyttöönottoon voi myös olla lähtökohdaltaan aivan toinen syy. Esimerkiksi yrityksen tarjoamia mobiililaitteita käytetäänkin vain yhden sovelluksen pyörittämiseen ja halutaan yksinkertaisesti hallita ajoittaista yhden sovelluksen päivitystä. On myös mahdollista, että mobiililaitetta halutaan käyttää vain niin sanottuna reitittimenä ja tässä tilanteessa halutaan vain ylläpitää laitepäivityksiä.

Insinöörityössä käytiin lävitse MDM:n perusteita ja käsitteitä sekä sitä, mitä tulisi ottaa huomioon MDM-ratkaisua valittaessa. Työn tavoitteena oli löytää ratkaisu siihen, miten Medixine kykenisi hallitsemaan ja seuraamaan Medixinen asiakasyrityksille tarjoamia Android-pohjaisia mobiililaitteita. MDM-palveluiden kartoittamisen ja laajasta tarjonnasta kahteen kandidaattiin kohdistuneiden testikäyttöönottojen seurauksena lopputulemaksi tuli se, että Medixine tulee ottamaan käyttöön Microsoftin tarjoaman Intune MDM -ratkaisun.

MDM-ratkaisuvalinnan perusteluna oli yksinkertaisesti se, ettei Intunen käyttöönotto luonut yritykselle lainkaan lisäkuluja. Jos tulevaisuudessa tulisi vastaan tilanne, jossa Intunen osalta havaittaisiin puutteita kriittisien ominaisuuksien puolesta ja Sophos Mobile sisältäisi nämä puuttuvat ominaisuudet, voitaisiin mahdollisesti ottaa käyttöön Sophos Mobile rajoitetuin ominaisuuksin, sillä Sophos Mobile mahdollistaa API-integraation Microsoft Intunen kanssa. Tämä tarkoittaa käytännössä sitä, että vaikka yrityksen mobiililaitteet olisivat jo Microsoft Intunen piirissä, integraation ansiosta niitä päästäisiin hallitsemaan myös Sophos Mobilen puolella ja niihin voisi ottaa käyttöön Sophoksen mahdollisesti monipuolisemmat laite- ja mobiilihallintaominaisuudet. Tähän perustuen työn käytännönosuuden jälkeen

tullaan jatkamaan Intunen lisäksi myös Sophos Mobilen laajempaa tutustumista ja toiminnallisuuksien kartoittamista.

Ennen insinöörityön loppua saatiin vielä toteutettua Intunen kautta asetus- ja käytäntökokonaisuus, jolla mobiililaite saatiin asetettua Kiosk Modeen. Tämä rajoittaa mobiililaitteen käyttöjärjestelmäpuolen asetuksien, ominaisuuksien ja sovellusten käytön miltei täysin. Mobiililaitteeseen asennettiin DeviceHub-sovellus ja ensimmäiset mittaukset saatiin toteutettua onnistuneesti Medixine Suitessa.

Insinöörityön valmistumisen jälkeen projektin käytännönosuus tulee jatkumaan aktiivisena Medixinellä. Jatkossa tullaan toteuttamaan laitteiden liittämisen osalta massaliitostestejä siitä, miten usean mobiililaitteen ylläpito suoriutuu MDM-palvelussa.

Insinöörityössä ei ehditty tarpeeksi ottaa huomioon mahdollista turvallisuuspuolta Medixinen laitehallinta ja seurantatapaukseen liittyen. Tämä tullaan ottamaan työn alle ennen tuotantokäyttöönottoa.

Lähdettäessä toteuttamaan projektia MDM-ratkaisun löytämiseksi voidaan todeta käytännön työlle varattavan ajan jääneen liian vähäiseksi ja projektiin olisi pitänyt varata enemmän yhtäjaksoista työskentely aikaa MDM-ratkaisujen testaamiselle. Se, mitä insinöörityön aikana on opittu MDM-ratkaisujen testaamisen osalta, on että yksikään MDM-ratkaisu ei ole mikään yhden ominaisuuden sisältävä web-sovellus. Ominaisuuksia ja toiminnallisuuksia löytyy jokaisesta MDM-ratkaisusta aivan valtava määrä. Ennen kuin lähdetään kartoittamaan vaihtoehtoja, tulisi tarkkaan miettiä ja suunnitella myös tulevaisuuden osalta, mitä halutaan vaatia MDM-ratkaisulta.

Lähteet

1 Top 5 Reasons Why Enterprise Needs Mobile Device Management. 2021. Verkkoaineisto. <https://www.wirelesswatchdogs.com/blog/top-5-reasons-why-enterprise-needs-mobile-device-management>. Luettu 24.10.2021.

2 IBM.com, What is Mobile Device management. 2021. Verkkoaineisto. <https://www.ibm.com/topics/mobile-device-management>. Luettu 20.7.2021.

3 Medixine Oy. 2021. Medixine lyhyesti. Verkkoaineisto. <https://www.medixine.fi/yritys/>. Luettu 6.4.2021.

4 Teinonen, Otto. 2021. CTO. Medixine Oy. Haastattelu Medixine tiloissa. Medixine DeviceHub historia ja tausta + Medixine Suite perusteet. 7.4.2021.

5 Sinivirta, Mikko. 2021. Medixine Oy yleisöanti 5.8.-4.9.2020. Verkkoaineisto. <https://www.sijoitustieto.fi/profiili/Mikko%20Sinivirta/viimeisimmat-viestit>. Luettu 23.10.2021.

6 Medixine Oy. 2021. Screening and Follow-up of Coronavirus (COVID-19). Verkkoaineisto. <https://medixine.com/coronavirus/>. Luettu 23.10.2021.

7 Relander, Peter. 2021. Business Controller. Medixine Oy. Haastattelu Teams-palaverissa. Medixinen taloustilanne ja lähitulevaisuuden näkymä yrityksen talouden näkökulmasta. 1.6.2021.

8 news.cision.com. 2021. Etälääketieteen alustan kehittänyt Medixine keräsi 2,9 miljoonan euron rahoituksen etähoidon tehostamiseen ja lisäämiseen. Verkkoaineisto. <https://news.cision.com/fi/san-francisco-oy/r/etalaaketieteen-alustan-kehittanyt-medixine-kerasi-2-9-miljoonan-euron-rahoituksen-etahoidon-tehosta,c3362787>. Luettu 1.8.2021.

9 Europe Telemedicine Market Research Report 2021 – 2026, Market Data Foroceast, elokuu 2021. Verkkoaineisto. <https://www.marketdataforecast.com/market-reports/europe-telemedicine-market>. Luettu 7.9.2021.

10 Steele, Colin. 2020. Mobile device management (MDM). Verkkoaineisto. <https://searchmobilecomputing.techtarget.com/definition/mobile-device-management>. Luettu 1.8.2021.

11 Shubham Pathak. 2019. Mobile Threat Defense (MTD): What Companies Should Know. Verkkoaineisto. <https://blog.scalefusion.com/mobile-threat-defense-what-companies-should-know/?utm_source=blog&utm_medium=What%20is%20MDM%3F%20Mobile%20Device%20Management%20Software%20%7C%20Scalefusion%20Blog&utm_campaign=Scalefusion%20Blog>. Luettu 20.9.2021.

12 ManageEngine. 2021. Mobile Application Management (MAM). Verkkoaineisto. <https://www.manageengine.com/mobile-device-management/mobile-application-management.html>. Luettu 15.10.2021.

13 VMware. 2021. What is Unified Endpoint Management (UEM). Verkkoaineisto. <https://www.vmware.com/topics/glossary/content/unified-endpoint-management>. Luettu 23.10.2021.

14 SysGen experience IT. 2020. 3 Reasons Your Business Needs MDM. Verkkoaineisto. <https://sysgen.ca/3-reasons-business-needs-mdm/>. Luettu 7.9.2021

15 Buch, Nema. 2018. Research and Marketing professional. 7 Important Factors to Consider When Choosing an MDM Solution. Verkkoaineisto. <https://blog.scalefusion.com/7-important-factors-to-consider-when-choosing-an-mdm-solution/>. Luettu 7.8.2021.

16 Duo Security. 2021. 10 thing to consider before buying an MDM Solution. Verkkoaineisto. <https://cdn2.hubspot.net/hubfs/2283880/ten-things-to-consider-before-buying-an-mdm-solution-2.pdf>. Luettu 30.10.2021.

17 Microsoft Intune. 2021. Intune Documentation. Verkkoaineisto. <https://docs.microsoft.com/en-us/mem/intune/>. Luettu 24.7.2021.

18 Microsoft Intune architecture. 2020. High-level architecture for Microsoft Intune. Verkkoaineisto. <https://docs.microsoft.com/en-us/mem/intune/fundamentals/high-level-architecture>. Luettu 20.10.2021.

19 Microsoft Community Site. 2021. Intune Community. Verkkoaineisto. <https://techcommunity.microsoft.com/t5/microsoft-intune/bd-p/Microsoft-Intune>. Luettu 1.10.2021.

20 Microsoft Intune MAM. 2021. What is Microsoft Intune app management?. Verkkoaineisto. <https://docs.microsoft.com/en-us/mem/intune/apps/app-management>. Luettu 24.7.2021.

21 Microsoft docs. 2021. Enterprise Mobility + Security documentation. Verkkoaineisto. <https://docs.microsoft.com/en-us/enterprise-mobility-security/>. Luettu 20.10.2021.

22 What is Azure resource manager. 2021. Verkkoaineisto. <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/overview>. Luettu 23.10.2021.

23 Embrace proactive security with Zero Trust. 2021. Zero Trust Maturity Model. Verkkoaineisto. <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT>. Luettu 23.10.2021.

24 Microsoft Intune User Help, Why Enroll Your Android device, 2020. Verkkoaineisto. <https://docs.microsoft.com/en-us/mem/intune/user-help/why-enroll-android-device>. Luettu 28.8.2021.

25 Microsoft Intune documentation. 2021. Enroll Android Device. Verkkoaineisto. <https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll>. Luettu 7.9.2021.

26 Common questions and answers with device policies and profiles in Microsoft Intune. 2021. How long does it take for devices to get a policy, profile, or app after they are assigned?. Verkkoaineisto. <https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-troubleshoot#how-long-does-it-take-for-devices-to-get-a-policy-profile-or-app-after-they-are-assigned>. Luettu 10.10.2021.

27 Sophos Mobile. 2021. Sophos Mobile user documentation. Verkkoaineisto. <https://docs.sophos.com/esg/smc/9-6/admin/en-us/esg/Sophos-Mobile/concepts/Welcome.html>. Luettu 10.9.2021.

28 Retirement calendar for Sophos Mobile products and apps. 2021. Verkkoaineisto. <https://support.sophos.com/support/s/article/KB-000035304?language=en_US>. Luettu 22.10.2021.

29 Sophos Mobile documentation. 2021. Enroll Android Devices. Verkkoaineisto. <https://docs.sophos.com/esg/smc/9-6/admin/en-us/esg/Sophos-Mobile/concepts/AddDevices.html>. Luettu 1.10.2021.

30 Sophos Mobile. 2021. Sophos Mobile factsheet. Verkkoaineisto. <https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophosmobilecontroldsna.pdf>. Luettu 15.10.2021.