VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Mika Isosalo

DIGITAALISEN RAPPUNÄYTÖN ETÄHALLINTA

Tekniikka
2021

VAASAN AMMATTIKORKEAKOULU
Tekniikka

TIIVISTELMÄ

Tekijä	Mika Isosalo
Opinnäytetyön nimi	Digitaalisen rappunäytön etähallinta
Vuosi	2021
Kieli	suomi
Sivumäärä	47
Ohjaaja	Jukka Matila

Opinnäytetyö tehtiin kiinteistötiedonhallintaan erikoistuneen startup-yrityksen toimeksiannosta. Työ sisälsi laitteiden testausta, ominaisuuksien kehittämistä ja uusien ratkaisuiden etsimistä. Etähallintajärjestelmän kehittämisen suurin motiivi oli mahdollistaa asiakkailla olevien rappunäyttöjen paremman hallinnan. Rappunäytöille ei ollut hallintajärjestelmää ja vikatilanteet vaativat aina käynnin vikakohteessa.

Tutkimustyön aikana tutustuttiin erilaisiin etähallintaratkaisuihin ja yhteyden muodostamiseen laitteeseen, joka sijaitsee toisessa verkossa. VPN-yhteyden avulla saatiin muodostettua yhteys laitteisiin internetin yli.

Työn aikana saatiin toteutettua etähallinta yrityksen käyttämiin rappunäyttölaitteisiin. Järjestelmä koostuu kahdesta erilaisesta tavasta muodostaa yhteys laitteeseen sekä hallintaan. Laitteiden käyttöjärjestelmän erilaisuuden vuoksi, sama ratkaisu ei onnistunut molemmissa laitteissa. Keskitetty hallintajärjestelmä molemmille järjestelmille on tulevaisuudessa yrityksen kehitysprojekti.

Avainsanat atk-laitteet, verkot (järjestelmät), järjestelmäsuunnittelu, sähköinen julkaisutoiminta

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietotekniikka

ABSTRACT

Author	Mika Isosalo
Title	Digital Signage Remote Control
Year	2021
Language	Finnish
Pages	47
Name of Supervisor	Jukka Matila

The thesis was done for a start-up company specialized in property management. The thesis involved the testing of different devices, developing features, and finding for new solutions. The main motive for developing remote management solution for devices was to be able to manage devices which customers have. There was no management system for the staircase displays and fault situations required a visit to the fault site.

During the research process various remote management solutions and other methods to connect to devices were tested. The VPN connection was one solution to control devices over the internet.

The main aim was attained with two different methods. The staircase displays managed by the company can now be controlled remotely. The system involves two separate solutions. The same solution with two devices was not possible due to different operation systems. A centralized management system will be a development project for the company in the future.

Keywords Computing devices, networks (systems), system design, electronic publishing

SISÄLLYS

KUVALUETTELO

TERMIT JA LYHENTEET

VPN	Virtual Private Network, virtuaalinen yksityinen verkko.
L2TP	Layer 2 tunneling protocol, tason kaksi tunnelointi protokolla.
VPS	Virtual Private Server, virtuaalinen yksityinen palvelin.
SSH	Secure shell, konsoli etäyhteys salatulla protokollalla.
ADB	Android Debug Bridge, Android virheenkorjaus.
REST	Representational State Transfer, arkkitehtuurimalli ohjelmointirajapintojen toteuttamiseen.
API	Application programming interface, ohjelmointirajapinta tiedonvälittämiseen.
HTTP	Hypertext Transfer Protocol, hypertekstin siirtoprotokolla.
HTTPS	Hypertext Transfer Protocol Secure, hypertekstin suojattu siirtoprotokolla.
WSS	Web services security, verkkopalveluiden lisäosa turvallisuuden parantamiseen.
HTML	Hypertext Markup Language, kieli, jolla käyttöliittymä ohjelmoitu.
PFS	Perfect Forward Secrecy, protokolla avaimien turvalliseen hallintaan.
HSTS	HTTP Strict Transport Security header, käskee verkkoselaimia käyttämään HTTPS yhteyttä.
TLS	Transport Layer Security, siirtoprotokolla turvalliseen tiedon välittämiseen.
MDM	Mobile Device Management, mobiililaitteen hallinta.
RSA	Public-key cryptosystem, julkisen avaimen salausjärjestelmä.
AES	Advanced Encryption Standard, edistynyt salaus standardi.
Kiosk	Näytön esittelytila missä sallitaan ainoastaan halutut toiminnot ja sovellukset.
APK	Android-sovellustiedosto
Pro mode	Ammattikäyttöön tarkoitettu laitteen lisäominaisuusvalikko.
IP	Internet Protocol, verkko-osoite
ovpn	Tiedostomuoto VPN asetuksien käyttämiseen eri laitteilla.
Cloud	Pilvipalvelin
KVM	Kernel-pohjainen virtuaalinen tietokone
Root	Järjestelmäkäyttäjä, jolla on laitteen täysi hallintaoikeus
Skripti	Komentojen suorittamista varten kirjoitettu ohjelma

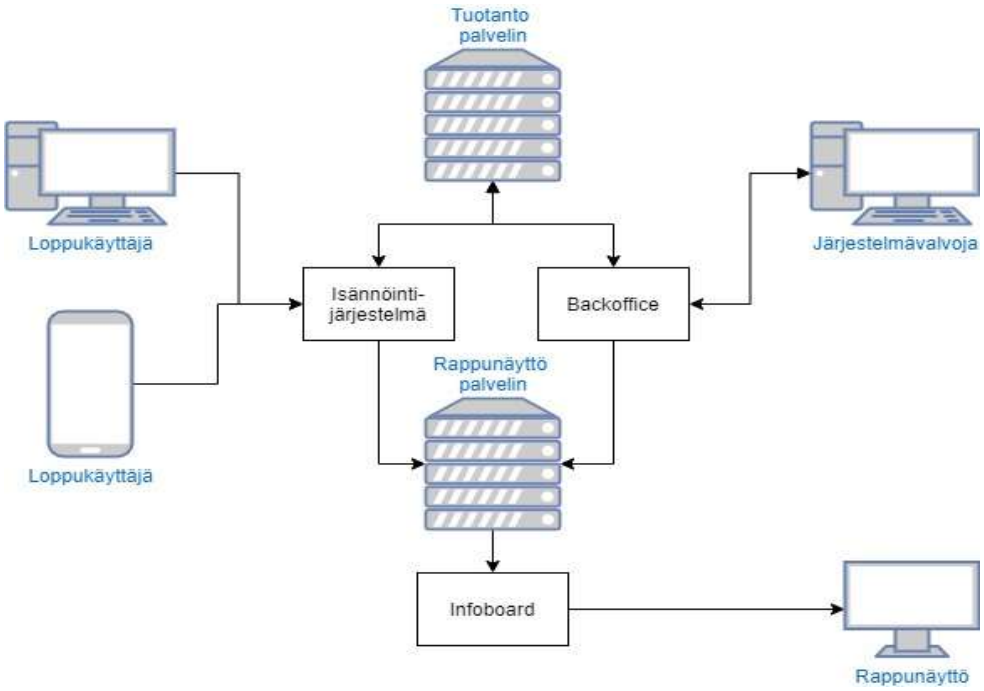
1 JOHDANTO

Opinnäytetyön tarkoituksena oli tutkia erilaisia etähallintaohjelmistoja ja järjestelmiä, joiden avulla voidaan toteuttaa toimeksiantajayritykselle digitaalisen sisällön esittäminen halutuissa käyttökohteissa. Yritys tarjoaa asiakkailleen rappunäyttöpalvelua, jonka avulla taloyhtiöissä voidaan esittää tarpeellista ja ajankohtaista tietoa jokapäiväisessä toiminnassa. Tarpeellinen tieto on esimerkiksi tärkeimmät yhteystiedot, asunto- ja asukasluettelo sekä tärkeimmät informatiiviset tiedotteet koskien taloyhtiön toimintaa.

Työssä keskitytään kehittämään toimiva järjestelmä yrityksen olemassa olevia laitteita hyödyntäen sekä uusia käyttötarkoitukseen sopivia laitteita liittämällä. Järjestelmässä tullaan käyttämään kahta erilaista käyttötarkoitukseen sopivaa näyttöä, reititintä sekä useaa eri virtuaalista palvelinta.

2 JÄRJESTELMÄN JA LAITTEIDEN YLEINEN KUVAUS

Tässä luvussa käydään läpi tutkimustyöhön liittyvän järjestelmän yleistä kuvausta ja siihen kuuluvia tärkeimpiä osa-alueita. Luvuissa kolme, neljä ja viisi käydään tarkemmin läpi tutkimustyönaikana suoritettua teknistä toteutusta.



Kuva 1. Järjestelmän yleinen kuvaus.

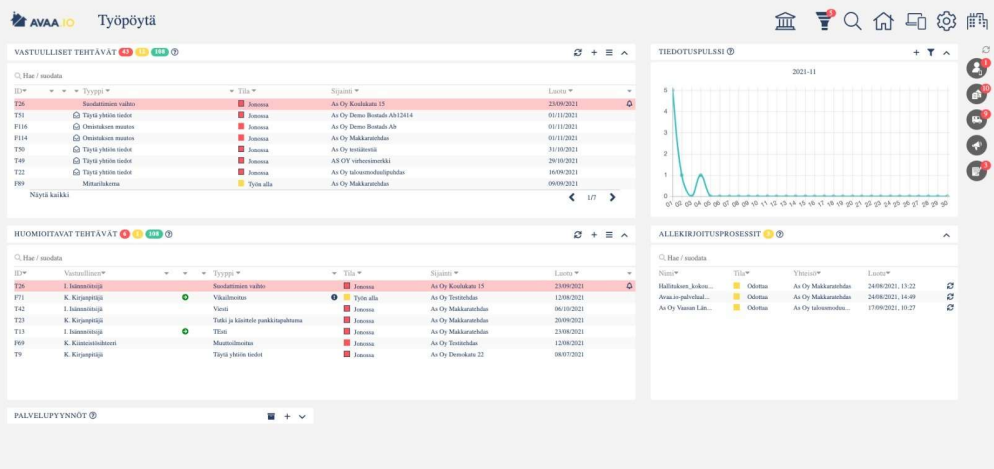
Tutkimustyöhön liittyviä palvelimia kuuluu yhteensä kaksi kappaletta. Kuvassa 1 kuvataan järjestelmää ja näytetään millä tavalla palvelimet ja palvelut ovat yhdistetty toisiinsa. Järjestelmään kuuluu tuotanto ja rappunäyttöpalvelimet. Jokainen palvelin on erillinen virtuaalinen tietokone, joka on ostettu ulkoiselta palveluntarjoajalta.

2.1 Tuotantopalvelin

Tuotanto-palvelin on järjestelmän tärkein ja suurin osuus. Palvelimella on kiinteistötiedonhallinta-alusta mikä toimii sisällöntuottajana myös rappunäyttöihin.

Alusta jakautuu kahteen suurempaan osioon, editoriin ja BackOfficeen. Palvelu on rakennettu soveltamalla avoimen lähdekoodin pohjajärjestelmiä.

BackOffice toimii järjestelmänvalvojan hallintatyökaluna. Alustan kautta hoidetaan ylläpidollisia asioita, jotka vaikuttavat editoriin. Järjestelmävalvoja voi lisätä uusia isännöintitoimistoja, hallita taloyhtiöiden asetuksia hallinta-alustalle sekä hallita rappunäyttöjen käyttäjiä. Editoriin tehtävät päivitykset ja ominaisuuksien aktivoiminen ja deaktivoiminen tehdään BackOfficen kautta.

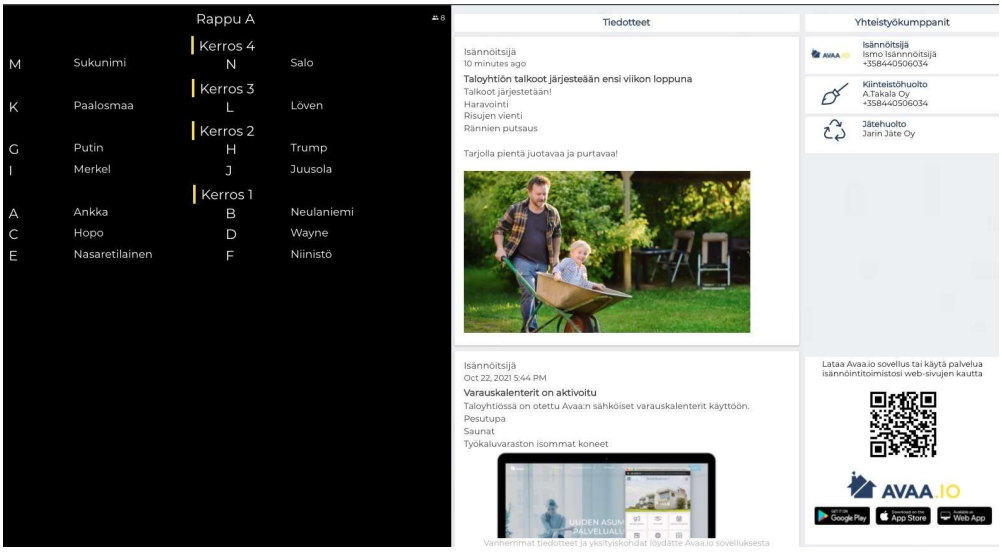


Kuva 2. Kiinteistötiedon hallinta-alustan käyttöliittymä.

Kuvassa 2 on editori eli hallinta-alusta, joka toimii kiinteistöjen hallintaan. Hallinta-alustan kautta asiakkaana olevat isännöintitoimistot ja heidän henkilökuntansa voivat hallita kiinteistöjä sekä taloyhtiöitä. Alustan kautta voidaan hallita kaikkea taloyhtiön arkeen liittyviä asioita, esimerkiksi vikailmoituksia, tiedottamista, osakas- ja asukasrekisteriä. Palvelimien välille on tehty rajapintayhteyksiä, joiden avulla tieto kulkee vaivattomasti niihin paikkoihin mihin tieto tulee välittää. Rappunäytöt ovat yksi tämän alustan ominaisuuksia, johon editorissa tehtävät muutokset päivittävät tietoa.

2.2 Rappunäyttöpalvelin

Rappunäyttöpalvelimelle on tehty selainpohjainen rappunäyttösovellus. Selainpohjaista sovellusta voidaan käyttää minkä tahansa selaimen kautta tai Android-pohjaisen sovellustiedoston kautta. Tämän sovelluksen voi asentaa Android-TV:hen tai tavalliseen Android-käyttöjärjestelmään. Näyttö voidaan asettaa vaaka- tai pystysuuntaisesti. Kuvassa 3 on vaakatasoisen rappunäytön näkymä.



Kuva 3. Selainpohjainen rappunäyttö.

Pystysuuntaisessa asettelussa on kosketusominaisuuksia. Kosketuksella voidaan mahdollistaa arkistoitujen tiedotteiden lukeminen, lomakkeiden täyttäminen, tärkeimpien yhteystietojen hakeminen sekä varauskalenterin hyödyntäminen taloyhtiön tarjoamille palveluille ja tiloille.

Tuotanto- ja rappunäyttöpalvelimen väliin on tehty rajapintayhteys minkä avulla näytön tietoja voidaan päivittää kiinteistötiedonhallinta-alustapalvelun kautta.

3 ETÄHALLINTA JA OHJAUS

Tässä luvussa käydään läpi yleisellä tasolla erilaisia etähallintaohjelmistoja. Testataan eri ohjelmien hyviä ja huonoja puolia, sekä puhutaan tietoturvallisuudesta yleisellä tasolla. Ohjelmistot on valittu siten, että niitä on mahdollista käyttää Android-käyttöjärjestelmän ohjaamiseen ja hallintaan. Testaamiseen käytetään 24 tuumaista kosketusnäyttöä, jonka käyttöjärjestelmänä on Android 8. Laite on suunnattu yrityksille, jotka haluavat tarjota digitaalista sisältöään erilaisissa käyttöympäristöissä. Käyttöjärjestelmä on valmiiksi rootattu eli käyttäjällä on täysi hallinta laitteeseen.

Testiin valitut ohjelmistot on suunniteltu MDM käyttöön. Lyhenne tulee englanninkielisistä sanoista Mobile Device Management eli mobiililaitteiden hallinta. Kriteereinä ohjelmalle oli laitteen ominaisuuksien rajoittaminen, oman sisällön näyttäminen ja hallinta sekä helppokäyttöisyys.

Aikaisemman kehitysprosessin aikana Android-laitteet osoittautuivat käyttökokemuksen puolesta parhaimmaksi vaihtoehdoksi. Vertailukohteena on käytetty Raspberry PI-laitetta koskeutusnäytön kanssa sekä kosketusnäytöllistä tietokonetta, johon oli asennettu Linux-käyttöjärjestelmä. Laitteen koko ja kosketuksellisen käyttöjärjestelmän toimivuus kallistui Androidin puolelle.

3.1 Testauksen suunnitelma

Testausta varten laadittiin suunnitelma, miten laitteen ja järjestelmän tulee toimia. Tämän suunnitelman kriteereitä noudatettiin ohjelmistojen testauksessa. Kriteerit ovat taulukossa 1. Jokaista ohjelmaa testattiin kahden viikon ajan. Laite oli päällä koko tämän testijakson. Kriteereitä testattiin useita kertoja ja niiden lopputulokset on listattu jokaista ohjelmistoa koskevassa testauskappaleessa.

Taulukko 1. Testauksen kriteerit ohjelmistolle.

Kohta	Selite
1.	Rappunäyttö sovelluksen tulee käynnistyä automaattisesti laitteen käynnistyessä sekä palautua sovellukseen, mikäli siitä onnistutaan poistumaan.
2.	Laitteen kautta ei saa pystyä muuttamaan mitään asetuksia mukaan lukien verkon asetuksia, näytön asetuksia tai muita laitteen asetuksia.
3.	Sovelluksen vaihtaminen tai muun sovelluksen kuin rappunäyttösovelluksen avaaminen tulee estää.
4.	Laitteen näytön tulee pysyä päällä vuorokauden ympäri.
5.	Etähallinnan kautta pitää pystyä käynnistämään laite uudestaan.
6.	Etähallinnan kautta pitää pystyä päivittämään sovellus.
7.	Etähallinnan kautta olisi hyvä pystyä käyttämään laitetta kuin sitä käyttäisi fyysisesti.

3.2 AirDroid

AirDroid on vuonna 2011 alkunsa saanut etähallintaohjelmisto, jonka tarkoituksen on helpottaa puhelimen ja tietokoneen välistä tiedonsiirtoa ja hallintaa. Ohjelmistoa voi käyttää langattoman sisäverkon tai internetin yli. Monipuoliset ominaisuudet mahdollistavat räätälöidyn järjestelmän, jonka avulla saadaan haluttu etähallinta. Seuraavissa kappaleissa tutustutaan AirDroid Businessin ominaisuuksiin. (Sand Studio, Airdroid about)

3.2.1 Turvallisuus

Järjestelmä käyttää etäyhteyden muodostamiseen TLS-tunnelia. Tunneli muodostetaan käyttämällä HTTPS- ja WSS-protokollaa. Yhteys todennetaan RSA-avainparilla. RSA-avainparissa yksityinen avain on käyttäjän tietokoneeseen tallennettuna ja julkinen avain on kohde laitteessa. Istunto salataan AES 256-bit salauksella. (Sand Studio, Airdroid Security)

3.2.2 Käyttökohteet

Laajojen ominaisuuksien puolesta ohjelmistoa voidaan hyödyntää Android-käyttöjärjestelmällä varustetuissa puhelimissa, tableteissa, mainosnäytöissä julkisissa tiloissa tai vaikka myymälöissä.

Kiosk-ominaisuutta käyttämällä laitteen sovelluksien käyttöä voidaan rajoittaa halutulla tavalla. Tässä tilassa valitaan sallitut sovellukset sekä voidaan myös rajoittaa mille internetsivustoille laitteella on mahdollista mennä. Tämä mahdollistaa laitteen käyttämisen vain siihen tarkoitukseen mihin se on hankittu.

3.2.3 Käyttöönotto

AirDroid Business käyttöönottaminen oli erittäin helppoa. Tilin luomisen jälkeen uuden laitteen lisääminen voidaan tehdä kahdella eri tavalla. Kohdelaitteeseen asennetaan hallintasivun kautta ladattu APK eli sovellustiedosto. Tämä sovellustiedosto asentaa sovelluksen laitteeseen ja se yhdistyy suoraan omaan asiakkuuteen. Toinen vaihtoehto on ladata sovellus hallintasivulla näkyvän linkin kautta suoraan kohdelaitteessa. Jälkimmäinen vaihtoehto on hieman helpompi, kun siinä ei tarvitse siirtää sovellustiedostoa laitteesta toiseen. Molemmissa vaihtoehdoissa pitää syöttää koodi, jonka jälkeen laite yhdistetään käyttöliittymään.

3.2.4 Testaus

Testauksen aikana kiosk-tilan määrittäminen onnistui helposti. Profiilien avulla saadaan nopeasti luotua konfiguraatio, minkä avulla laitteeseen saadaan asetukset synkronoitua vaivattomasti. Laite saatiin toimimaan profiilin avulla nopeasti. Hallintasivun kautta etäyhteyden ottaminen laitteeseen onnistuu ilman erillisiä hyväksymisvahvistuksia. Käyttöliittymästä näkee myös ”kuvakaappauksen” pienenä kuvana. Tästä näkee nopeasti, jos laitteessa on jonkinlainen vikatilanne päällä.

Etäohjaus ei kuitenkaan toimi aivan halutulla tavalla. Hiiren osoitin ja painallukset eivät osu kohdelaitteessa samaan kohtaan kuin etänäyttö antaa ymmärtää. Tämä tekee etähallinnasta hyödyttömän kyseisen laitteen kanssa.

Testaukselle asetetuista kriteereistä osa toteutui (**Taulukko 1.**)**.**

1. ONNISTUI - Rappunäyttösovellus käynnistyy automaattisesti uudelleenkäynnistyksen yhteydessä ja palautuu sovellukseen, mikäli siitä poistutaan.
2. EPÄONNISTUI – Laitteen yläpalkin kautta näkyviä asetuksia oli mahdollista nähdä ja muuttaa.
3. ONNISTUI - Valikon/ kotinäkymän sovelluksia voitiin rajoittaa niin, että vain rappunäyttösovellus näkyi listauksessa.
4. ONNISTUI - Laitteen näyttö pysyy käynnissä ympärivuorokautisesti.
5. EPÄONNISTUI - Etähallinnan kautta ei ole mahdollista käynnistää laitetta uudestaan.
6. ONNISTUI - Etähallinnan kautta on mahdollista päivittää sovellus lataamalla uusi versio.
7. EPÄONNISTUI - Etähallinnan kautta on teoriassa mahdollista käyttää laitetta livenäkymän kautta hiirellä. Tämä ei kuitenkaan toiminut oikealla tavalla.

3.3 ManageEngine Mobile Device Manager

Yritys on aloittanut toimintansa vuonna 1996 nimellä AdventNet. Päätoimiala on alusta asti ollut verkonhallinta. Vuonna 2002 ManageEnginestä tuli oma osasto osana Zoho-yhtiötä. ManageEngine tarjoaa erilaisia tietotekniikanalan työkaluja, joita yhtiöllä on enemmän kuin 90. Mobile Device Manager on yksi näistä työkaluista. (Zoho Corporation, ManageEngine about-us)

3.3.1 Turvallisuus

Laitteidenväliseen liikenteeseen käytetään TLS-salausta. Yhteyksien turvaamiseen käytetään myös PFS:ää, joka varmistaa, että vaikka palveluntarjoaja onnistuttaisiin hakkeroimaan, ei aikaisempia istuntoja voida purkaa. Ainoastaan käynnissä oleva istunto vaarantuu.

Palveluntarjoaja on aktivoinut HSTS:n viestittämään selaimelle, että yhteyden voi avata ainoastaan suojatun yhteyden avulla. Tämä tarkoitta sitä, että ainoastaan HTTPS-protokolla voidaan käyttää yhteyden muodostamiseen.

Asiakkaiden arkaluontoinen data on suojattu 256-bittisellä AES-suojauksella. Salattujen tiedostojen salausavaimet suojataan lisäksi toisella avaimella. Nämä avaimet sijaitsevat erillään muista salausavaimista toisella palvelimella. (Zoho Corporation, ManageEngine Security)

3.3.2 Käyttökohteet

Järjestelmä tukee useita eri käyttöjärjestelmiä ja laitteita. Tuetut käyttöjärjestelmät/laitteet ovat iOS/iPadOS, macOS, Android, Samsung, Windows Phone, Windows Laptop, Chrome OS ja tvOS. Järjestelmää voi hyödyntää yrityksien puhelimien ja tietokoneiden sekä julkisiin tiloihin asennettavien laitteiden hallintaan. Kiosk-ominaisuus mahdollistaa julkisissa tiloissa olevien laitteiden halutun käyttötavan ja tarkoituksen.

3.3.3 Käyttöönotto

Mobile Device Managerin asentaminen laitteeseen tapahtuu käyttämällä ”makedeviceowner.bat”-tiedostoa. Skriptin avulla sovellukselle määritetään laiteomistajan oikeudet. Skriptissä suoritetaan kaksi komentoa. Komennot näkyvät kuvassa 4.

```
adb.exe install -r MDMAndroidAgent.apk
adb.exe shell dpm set-device-owner com.manageengine.mdm.android/com.manageengine.mdm.framework.deviceadmin.DeviceAdminMonitor
```

Kuva 4. Makedeviceowner.bat skripti (Zoho Corporation, ManageEngine Device Owner).

Ensimmäinen komento asentaa laitteeseen sovelluksen ja toinen komento määrittää sovelluksen laitteen omistajaksi (Zoho Corporation, ManageEngine Device Owner). Skriptin suorittamisen jälkeen seurataan hallintasivun ohjeita laitteen lisäämiseksi. Sovellukseen syötetään kertaluonteiset verkko-osoite ja salasana. Lisäksi syötetään haluttu käyttäjätili.

Laiteprofiilin avulla voidaan määrittää laitteelle omat asetukset, rajoitukset sekä sovellukset. Profiilit voidaan linkittää ryhmään ja laitteet liitetään haluttuun ryhmään, jonka jälkeen laitteet saavat oikeat määritykset. Tämä on nopea tapa lisätä uusia laitteita järjestelmään, kun on kerran tehnyt hyvän profiilin.

3.3.4 Testaus

Testauksessa kohdelaitteella ilmeni muutamia ongelmia. Asennus skriptin jälkeen sovellus ei toiminut oikein. Osoitteen syöttämisen jälkeen sovellus ei enää vastaanottanut vahvistuspainiketta. Ongelma saatiin kierrettyä, kun skriptin toinen komento suoritettiin vasta osoitteen kirjoittamisen jälkeen.

Toinen ongelma sovelluksen toimivuuden kanssa ilmeni kiosk-ominaisuuden kanssa. Tilaa ei pystynyt käyttämään ilman, että hallintasovelluksen oma palkki näkyi näytöllä. Visuaalisesti tämä ei ollut hienon näköinen eikä sopinut rappunäyttöön. Lisäksi alapalkin kotipainiketta naputtamalla oli mahdollisuus siirtyä poiskirjautumiseen kiosk-tilasta. Ilman salasanaa ei kiosk-tilasta voi poistua, mutta poiskirjautumisikkuna jäi näkyviin niin pitkäksi aikaa, kunnes siitä poistuttiin manuaalisesti. Julkisessa tilassa olevan näytön kanssa tämä ei ollut hyväksyttävää.

Testaukselle asetetuista kriteereistä osa toteutui (**Taulukko 1.**).

1. EPÄONNISTUI - Rappunäyttösovellus käynnistyy automaattisesti uudelleenkäynnistyksen yhteydessä, mutta ei palaudu takaisin sovellukseen, mikäli onnistuu pääsemään ”poistu kiosk-tilasta”-valikkoon.
2. ONNISTUI – Laitteen asetuksia ei pystynyt muuttamaan kiosk-tilassa.
3. ONNISTUI - Valikon/ kotinäkymän sovelluksia voitiin rajoittaa niin, että vain rappunäyttösovellus näkyi listauksessa.
4. ONNISTUI - Laitteen näyttö pysyy käynnissä ympärivuorokautisesti.
5. ONNISTUI - Etähallinnan kautta on mahdollista käynnistää laite uudestaan.
6. ONNISTUI - Etähallinnan kautta on mahdollista päivittää sovellus lataamalla uusi versio.

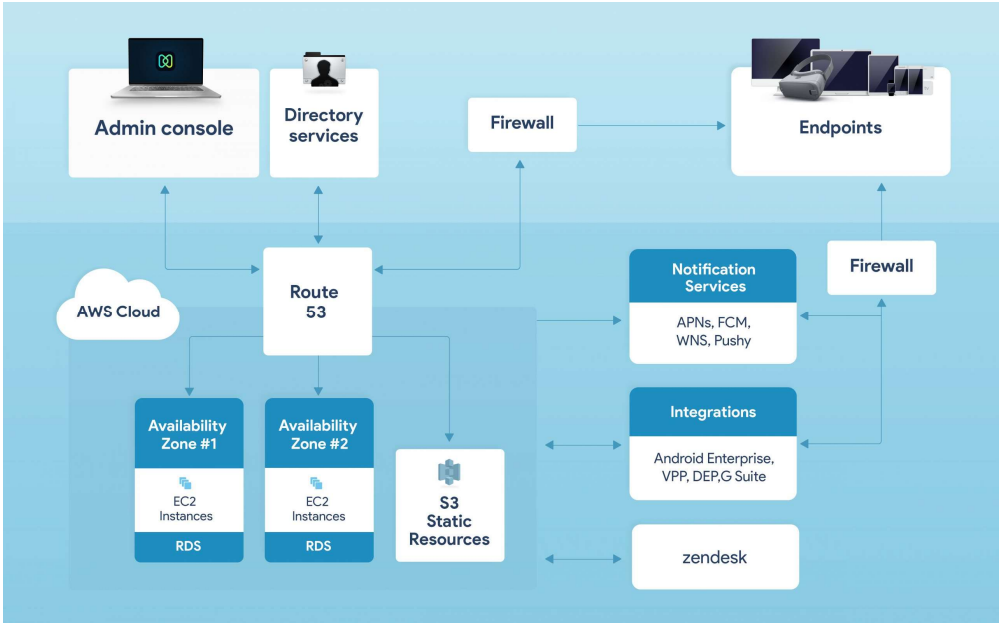
7. EPÄONNISTUI - Etähallinnan kautta ei pysty hallitsemaan laitetta etänä ilman, että hallintapyyntö vahvistetaan näytöltä fyysisesti.

3.4 Hexnode

Hexnode on maailmanlaajuisesti käytetty laajalle laitevalikoimalle tarkoitettu etähallintajärjestelmä. Palvelu tarjoaa monipuolisilla ominaisuuksilla varustetun hallintapaneelin, minkä avulla yrityksen laitteita voidaan hallita turvallisuus edellä. Hexnode mahdollistaa laitteiden ja sovelluksien päivittämisen saumattomasti yrityksen työntekijöiden laitteisiin. (Mitsogo Inc, Hexnode about-us)

3.4.1 Turvallisuus

Järjestelmä käyttää etäyhteyden muodostamiseen TLS-tunnelia. Tunneli muodostetaan käyttämällä HTTPS- tai WSS-protokollaa. Yhteys todennetaan RSA-avainparilla. RSA-avainparissa yksityinen avain on käyttäjän tietokoneeseen tallennettuna ja julkinen avain on kohdelaitteessa. Istunto salataan AES 256-bittisellä salauksella. (Mitsogo Inc, Hexnode security) Kuvassa 5 on arkkitehtuurikuva Hexnoden järjestelmästä.



Kuva 5. Arkkitehtuurikuva järjestelmästä (Mitsogo Inc, Hexnode Architecture).

3.4.2 Käyttökohteet

Hexnode tukee laajasti eri käyttöjärjestelmiä. Tämä mahdollistaa järjestelmän hyödyntämisen, melkein missä tahansa käyttötarkoituksessa. Tuetut käyttöjärjestelmät ovat: iOS, Android, Windows macOS, tvOS ja Fire OS.

Opinnäytetyön näkökulmasta tärkein vaatimus MDM-sovellukselle on mahdollistaa laitteen haluttu käyttötarkoitus julkisessa kohteessa ilman väärinkäytön mahdollisuutta. Väärinkäytön estämiseksi ainoastaan haluttu sovellus tulee olla mahdollista avata, laitteen asetuksien muuttaminen pitää estää ja laitteen tulee toimia automaattisesti. Rappunäyttösovelluksen tulee aueta automaattisesti käynnistymisen yhteydessä.

3.4.3 Käyttöönotto

Testauksen kohteena olevaan 24 tuumaiseen Android-laitteeseen asennettiin Hexnode For Work-sovellus. Tehtaalta toimitettuna laite on valmiiksi rootattu,

mikä mahdollistaa sovelluksen asentamisen laitteen omistajaksi. Tämä tarkoittaa, että sovellukselle annetaan laitteen täysi hallintaoikeus. Sovelluksen asentamiseen käytettiin ADB-yhteyttä Windows tietokoneen ja laitteen välillä. Asentamisen helpottamiseksi tehtiin lyhyt skripti, joka poistaa laitteesta tarpeettomat ohjelmat, muuttaa asetuksia, asentaa Hexnode For Work-sovelluksen ja määrittää sovelluksen laitteen omistajaksi.

```
:developer_settings

adb.exe shell "settings put global stay_on_while_plugged_in 1"
adb.exe shell "settings put global policy_control immersive.full=*"
echo.
echo Done
pause>nul
goto set_settings

:disable_applications
adb.exe shell "pm disable-user --user 0 com.elclcd.multifunctionclock"
adb.exe shell "pm disable-user --user 0 com.google.android.apps.maps"
adb.exe shell "pm disable-user --user 0 com.google.android.gm"
adb.exe shell "pm disable-user --user 0 com.android.gallery3d"
adb.exe shell "pm disable-user --user 0 com.google.android.syncadapters.calendar"
adb.exe shell "pm disable-user --user 0 com.android.calculator2"
adb.exe shell "pm disable-user --user 0 com.android.calendar"
adb.exe shell "pm disable-user --user 0 com.android.camera2"

echo.
echo Done
pause>nul
goto set_settings
```

Kuva 6. Asennusskriptin osa.

Kuvassa 6 on kuvakaappaus skriptin osasta mihin on määritetty Android-laitteen kehittäjäasetuksia kohdassa ”developer_settings”. Asetuksilla määritetään laite pysymään aina päällä laturin ollessa kytkettynä ja piilotetaan järjestelmä ylä- ja alapalkki, jolloin sovellus on aina koko näytössä. Kohdassa ”disable_applications” poistetaan laitteessa olevia sovelluksia, joita ei tulla käyttämään missään vaiheessa. Sovelluksia poistamalla estetään tarpeettomien sovelluksien päivittyminen tulevaisuudessa.

```
:install_hexnode
adb.exe install HexnodeForWork.apk
adb.exe shell "dpm set-device-owner com.hexnode.mdm.work/com.hexnode.mdm.receivers.HexnodeDeviceAdminReceiver"
echo.
echo Hexnode is installed
set /p choice= Do you want to open Hexnode? (y/n):
if '%choice%'=='y' adb.exe shell monkey -p com.hexnode.mdm.work -c android.intent.category.LAUNCHER 1
pause>nul
echo Continue....
pause>nul
goto menu
```

Kuva 7. Asennusskriptin toinen osa.

Kuvassa 7 näkyy Hexnode for work-sovelluksen asennusvaiheet. Kuvan 7 rivillä 3 on komento mikä määrittää sovelluksen laitteen omistajaksi. Asennuksen jälkeen käyttäjältä kysytään, halutaanko sovellus avata asennuksen viimeistelyksi. Asennus viimeistellään seuraamalla sovelluksen vaiheita.

3.4.4 Testaus

Sovelluksen asentamisen jälkeen muut laitteelle tehtävät määritykset voidaan tehdä Hexnoden hallintapaneelissa. Hallintapaneelissa voidaan määrittää erilaisia käytäntöjä. Käytäntöjen avulla laiteeseen määritetään esiasetetut asetukset, sovellukset, toiminnot ja rajoitukset. Käytäntöjen liittäminen ryhmiin mahdollistaa esimerkiksi asetuksien muuttamisen tai sovelluksen päivittämisen kaikkiin ryhmään kuuluville laitteille samanaikaisesti.

Käytäntöjen avulla laite saatiin käyttäytymään halutulla tavalla. Laite saatiin käynnistymään kiosk-tilaan automaattisesti. Tämä tila avaa rappunäyttösovelluksen automaattisesti. Mikäli sovellus kaatuu tai siitä pääsee poistumaan, avautuu sovellus uudestaan pienellä viiveellä. Tässä tilassa vain rappunäyttösovellus on sallittu, eikä laitteessa pysty muuta sovellusta avaamaan. Sovelluksen päivittäminen toimi testauksen aikana hyvin. Hallintapaneeliin ladattiin uusi versio sovelluksesta ja se päivittyi laitteeseen muutaman minuutin viiveellä. Laitteessa se näkyi siten, että sovellus sulkeutui ja avautui hetken päästä uudestaan.

Hexnoden huonoin puoli osoittautui olevan etäohjaus ja näytön katseleminen etänä. Sovelluksessa on mahdollista ottaa etäyhteys haluttuun laitteeseen. Yhteyden muodostaminen ei ole kuitenkaan mahdollista ilman, että kohde laitteesta vahvistetaan etäyhteyden salliminen. Haluttuun käyttötarkoitukseen tämä on pieni ongelma. Esimerkiksi jos sovelluksen välimuisti tyhjenee vikatilanteessa tai sovelluksen päivittyessä, ei sovellus enää pysty näyttämään rappunäytön tietoja. Tilanne vaatii uudelleenkirjautumisen sovellukseen, mutta tätä ei voida etänä tehdä nykyisessä sovelluksessa.

Testaukselle asetetuista kriteereistä osa toteutui (**Taulukko 1.**).

1. ONNISTUI - Rappunäyttösovellus käynnistyy automaattisesti uudelleenkäynnistyksen yhteydessä, ja palautuu takaisin sovellukseen, mikäli sovelluksesta poistutaan.
2. ONNISTUI – Laitteen asetuksia ei pystytty muuttamaan kiosk-tilassa.
3. ONNISTUI - Valikon/ kotinäkymän sovelluksia voitiin rajoittaa niin, että vain rappunäyttösovellus näkyi listauksessa.
4. ONNISTUI - Laitteen näyttö pysyy käynnissä ympärivuorokautisesti.
5. ONNISTUI - Etähallinnan kautta on mahdollista käynnistää laite uudestaan.
6. ONNISTUI - Etähallinnan kautta on mahdollista päivittää sovellus lataamalla uusi versio.
7. EPÄONNISTUI - Etähallinnan kautta ei pysty hallitsemaan laitetta etänä ilman, että hallintapyyntö vahvistetaan näytöltä fyysisesti.

3.5 Yhteenveto

Yksikään testatuista ohjelmistoista ei ollut täydellinen ja jokaisessa ohjelmistossa oli hyvät sekä huonot puolensa. Asennusprosessissa oli myös paljon eroja ohjelmistojen välillä. Ainoastaan AirDroid-ohjelmiston asentaminen oli helppo ja nopea

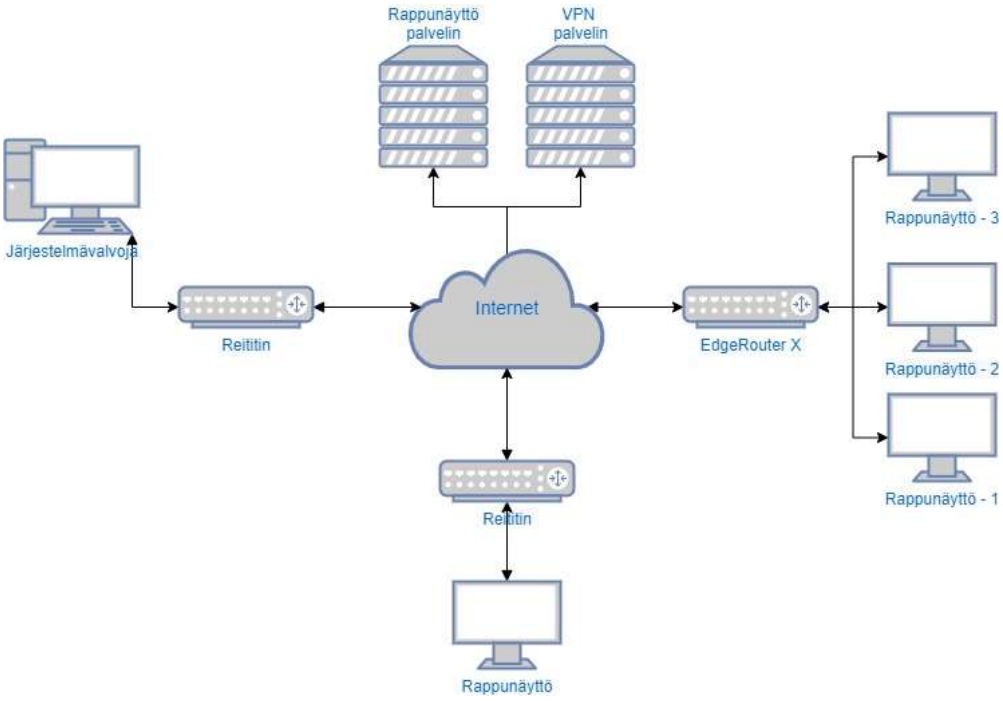
prosessi. Hexnode ja ManageEngine MDM-ohjelmistot vaativat enemmän aikaa ja perehtymistä, jotta asennuksesta saatiin mahdollisimman suoraviivainen prosessi.

Testauksen lopputuloksena Hexnode osoittautui parhaimmaksi vaihtoehdoksi, vaikka etähallinta ja etänäkymä eivät olleet mahdollisia ilman fyysistä vahvistusta laitteelta. Ohjelmisto täyttää muilta osin tärkeimmät kriteerit.

Lisäksi ohjelmisto tarjoaa rajapintakyselyiden tekemisen palvelimelta mitä ei testattu tässä työssä. Tulevaisuudessa rajapintakyselyiden tekeminen mahdollistaa tilatietojen tuomisen olemassa olevaan järjestelmään. Laitteiden seuranta ja osittainen hallinta voidaan toteuttaa paremmin, kun ei tarvitse kirjautua useaan eri järjestelmään. Profiilien hallinta ja sovelluksien päivittäminen on kuitenkin parempi toteuttaa Hexnoden oman hallintasivuston kautta.

4 ETÄHALLITTAVA RAPPUNÄYTTÖ

Opinnäytetyön aikana toteutettiin etähallintaohjaus kerrostalon rappunäyttöihin. Rappunäytöissä on taloyhtiön perustietoja, ilmoitustaulu sekä luettelo asunnoista ja asukkaista. Näyttö on ympärivuorokautisessa käytössä. Kuvassa 8 on järjestelmän rakenne. Näytöt muodostavat yhteyden rappunäyttö- ja VPN-palvelimelle. VPN-palvelin on tehty tutkimustyön aikana.



Kuva 8. Järjestelmän rakenne.

4.1 Taustaa ja vaatimukset

Etähallintaohjaus toteutettiin kohdeyrityksen toiminnassa olevaan rappunäyttöön. Näyttö on suunniteltu mainoskäyttöön ja sen ominaisuuksissa on mahdollista esimerkiksi käynnistää laite uudestaan tiettynä kellonaikana. Rappunäytön kanssa törmättiin usein ongelmiin, joissa sovellus ei ollut lähtenyt käyntiin ja näy-

tössä näkyi ainoastaan näytön kotivalikko. Ongelma ilmeni useasti ja vaikutti olevan yhteydessä internetyhteyteen. Kun näyttö putosi pois verkosta, myös sovellus kirjautui ulos eikä käynnistynyt uudelleen internetyhteyden palautuessa. Esiasetetun uudelleenkäynnistyksen jälkeen näyttö toimi halutulla tavalla. Alkuperäiset asetukset eivät mahdollistaneet tilan seurantaa paikallisen verkon ulkopuolelta.

Ongelmaan haluttiin löytää parempi ratkaisu, joka mahdollisti näytön turvallisen hallinnan etänä. Vaatimuksena on näytön sisällön muuttaminen sekä tärkeimpien ominaisuuksien, kuten uudelleenkäynnistäminen, näytön sammuttaminen ja päälle kytkeminen etäyhteyden avulla.

4.2 Laitteet

4.2.1 Rappunäyttö

Yrityksen käytössä oleva näyttö on Sonyn valmistama 43" ympärivuorokautiseen käyttöön tarkoitettu ammattinäyttö. Pääominaisuuksia on muun muassa etäohjaus REST APIilla sekä pro mode-valikko.

- Pro mode-valikon kautta voidaan määritellä erilaisia asetuksia, miten näyttö käyttäytyy. Oleellisimmat asetukset ovat sovelluksen aukaiseminen haluttuun tilaan, käytön rajoitukset (kukaan ei voi muuttaa näytön asetuksia ilman oikeaa salasanaa), fyysisten näppäimien ja kaukosäätimen käytön estäminen, sekä automaattisesti käynnistyminen ja sammuminen.
- Etäohjaus web APIn kautta on mahdollista toteuttaa samassa paikallisessa verkossa. REST API-komentoja voidaan lähettää yksinkertaisen HTML-sivun kautta missä määritellään näytön IP-osoite, salasana ja erilaiset komennot. Salasana määritetään TV:ssä verkon asetuksiin uuden näytön käyttöönottamisen yhteydessä. Komentojen lähettäminen ei ole mahdollista ilman salasanan syöttämistä. HTML-sivu ei käytä HTTPS-protokollaa, mutta käyttökohteessa muilla ei ole mahdollisuutta kirjautua verkkoon, joten tämä ei ole ongelma.

4.2.2 Reititin

Käyttökohteessa olevat näytöt olivat kytketty taloyhtiön omistamaan reitittimeen Ethernet-kaapeleilla. Reititin on ominaisuuksiltaan hyvin yksinkertainen eikä siinä ollut mahdollisuutta luoda VPN-yhteyttä.

Käyttökohteeseen valittiin uudeksi reitittimeksi kuvassa 9 näkyvä EdgeRouter X. Reititin on Ubiquitin valmistama 5 porttinen reititin, joka on erittäin monipuolinen reititin edulliseen hintaan verrattuna.

Kuva 9. EdgeRouter X.

Reititin määritettiin siten, että siihen on mahdollisuus ottaa etäyhteys VPN-yhteyden avulla. Tämä mahdollistaa sisäverkossa olevien rappunäyttöjen ohjauksen, kun yhteys on avattu. VPN-yhteys määritettiin käyttäen L2TP-protokollaa. Tämä vaihe on kuitenkin vain sitä varten, että voimme ottaa myöhemmin yhteyden suoraan reitittimeen ja muokata sen asetuksia. Myöhemmässä vaiheessa VPN-yhteys muutetaan siten, että etähallittavat laitteet ottavat yhteyden VPN-palvelimeen ja muu järjestelmä rakennetaan ottamaan yhteys VPN-palvelimeen, jolloin saamme laitteet yhdistettyä samalle palvelimelle. L2TP-yhteyden asetuksia ja palomuurisääntöjä tehdessä on käytetty reitittimen valmistajan ohjesivua L2TP-yhteyden määrittämiseen. (Ubiquiti, EdgeRouter X L2TP)

Turvallisuuteen liittyvät asiat huomioitiin reitittimen asennusvaiheessa. Oletuksena reititin sallii SSH-, HTTP- ja HTTPS-yhteyksien sisään tulevan liikenteen mistä tahansa IP-osoitteesta. Toisin sanoen nämä portit ovat oletuksena auki myös julkiseen verkkoon. Tämä on mahdollista estää muuttamalla ”listen-address” asetusta eli kuunteluosoitetta. Kuunteluosoitteeksi määritellään ne IP-osoitteet mistä halutaan sallia pääsy reitittimeen. Hallintasivulle voi mennä käyttämällä reitittimen IP-osoitetta, joko portin 80 tai 443 kautta. Molempien porttien pitäminen auki on tarpeeton, joten poistimme portin 80 asetuksista. Reitittimen sisäänpäin tulevaan liikenteeseen teimme muutoksia portteihin 22 ja 443. Näille porteille lisäsimme kuunteluosoitteeksi sisäverkon IP alueen kuvassa 10.

```
delete service gui http-port 80
set service gui listen-address 10.10.10.1
set service ssh listen-address 10.10.10.1
```

Kuva 10. EdgeRouter – asetukset komentoja.

```
#OpenVPN settings
set interfaces openvpn vtun0 config-file /config/auth/test_erx.ovpn
set interfaces openvpn vtun0 description 'OpenVPN VPN tunnel'
set service nat rule 5011 description 'masquarade for VPN'
set service nat rule 5011 log disable
set service nat rule 5011 outbound-interface vtun0
set service nat rule 5011 protocol all
set service nat rule 5011 type masquerade
```

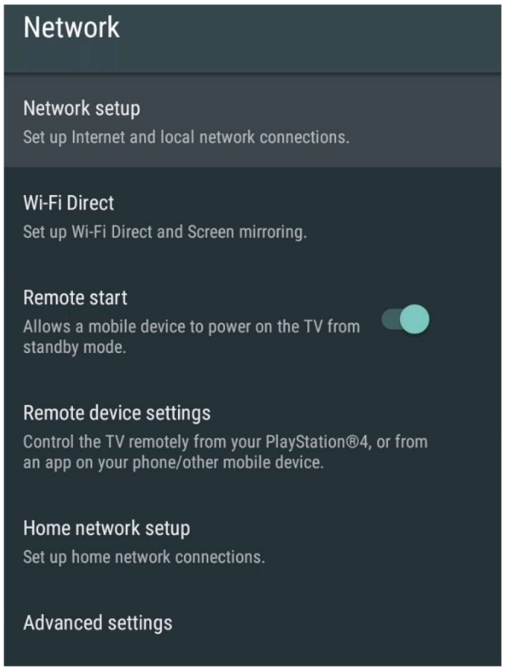
Kuva 11. EdgeRouter – VPN-komennot.

Kuvassa 11 määritetään asetukset OpenVPN-yhteyttä varten (Ryan Scullen, 2017 EdgeRouter X OpenVPN). Ovpn-tiedosto siirretään käyttämällä SCP-yhteyttä. Asetuksien myötä ainoastaan sisäverkosta voi päästä reitittimeen käsiksi tai VPN-yhteyden avulla.

4.3 Sony TV:n asetukset

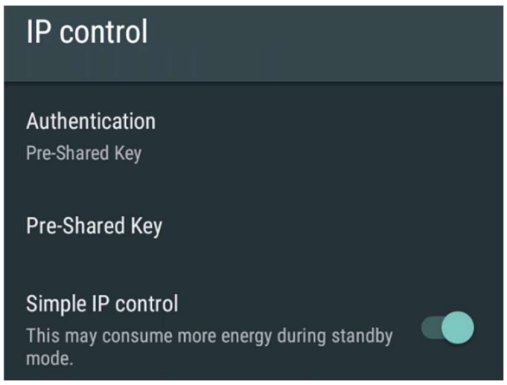
TV:n perusasetukset on määritelty valmiiksi ja tässä vaiheessa keskitytään asetuksiin, joilla määritetään laitteen käyttö julkisessa tilassa. Toiminallisuuksien rajoittaminen on välttämätöntä, jotta voidaan minimoida laitteen väärinkäyttö ja varmistaa haluttu käyttötarkoitus.

Verkkoasetuksista määritetään asetus mikä mahdollistaa tv:n ohjaamisen paikallisessa verkossa rajapinnan avulla. Kuvassa 12 verkon asetukset-valikko.



Kuva 12. Verkon asetukset.

Asetuksista määritetään kotiverkon asetukset ”home network setup”. IP-ohjauksella voidaan hallita laitetta. TV:n näytön voi sammuttaa tai laittaa päälle, vaihtaa sovellusta sekä tiedustella mikä sovellus on avoimena. Kuvassa 13 asetuksien määrittäminen IP-ohjaukselle.



Kuva 13. IP-ohjaus.

Ohjaus on suojattu omavalintaisella avaimella. Tämän avulla vain ne, jotka tietävät salasanan voivat hallita näyttöä.

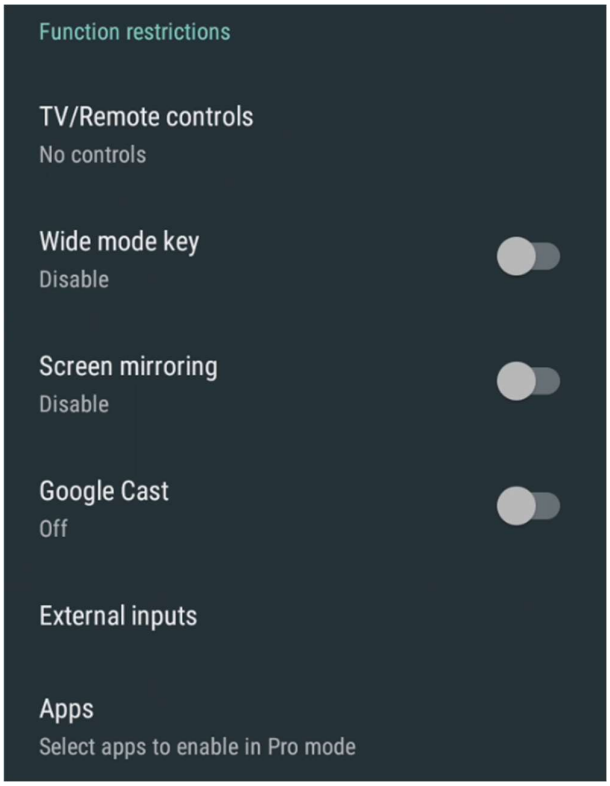
Pro mode-asetuksien kautta tehtävät määritykset:

- Rajoitetaan laitteen toiminnallisuuksia
- Määritetään käynnistyssovellus
- Määritettään API rajapintaetäohjaus
- Ajastetaan uudelleen käynnistyminen.

4.3.1 Toimintojen rajoittaminen

TV:n muita toiminto rajoitetaan myös mikä minimoi väärinkäytön mahdollisuuden. Pro mode-asetuksissa TV:n ja kaukosäätimen käyttö estetään. Tämä tarkoittaa sitä, että kaukosäätimen lähettämiä komentoja ei hyväksytä. Pro modesta poispääsemiseksi on kuitenkin määritelty näppäinyhdistelmä, jonka syöttämisen jälkeen voidaan aikaisemmin määritelty PIN-koodi syöttää. PIN-koodin syöttämisen jälkeen näyttö käynnistyy uudestaan ja asetuksia voi määrittää normaalisti kaukosäätimen avulla.

Ulkoiset tulolähteet (HDMI, AV/Component) on otettu pois käytöstä. Virtuaaliset tulolähteet, kuten näytön peilaaminen ja sisäänrakennettu Google Cast ominaisuudet, on myös estetty kuvassa 14.

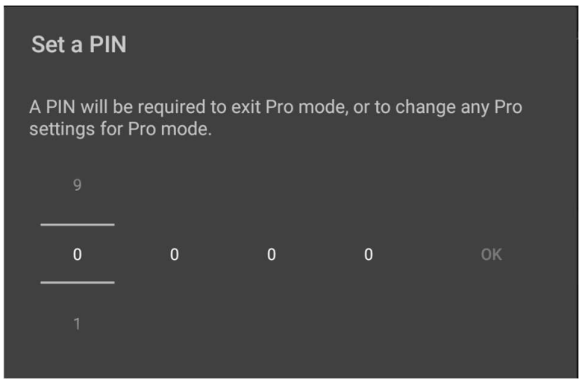


Kuva 14. Toimintojen rajoittaminen.

4.3.2 Lukitus

Yksi tärkeimmistä asetuksista on lukituksen määrittäminen. Lukituksen avulla suojataan pro mode-tilasta poistuminen. Lukitukseksi määritetään nelinumeroinen PIN-koodi. PIN-koodi voidaan syöttää kaukosäätimellä, vaikka kaukosäätimen käyttö estetään asetuksilla. Koodin pääsee syöttämään sen jälkeen, kun kaukosäätimellä on painanut näppäinyhdistelmä ”info, mykistys, - äänenvoimakkuus, koti”. Kuvassa 15 pro mode-lukituksen aktivointi ja kuvassa 16 PIN-koodin määrittäminen.

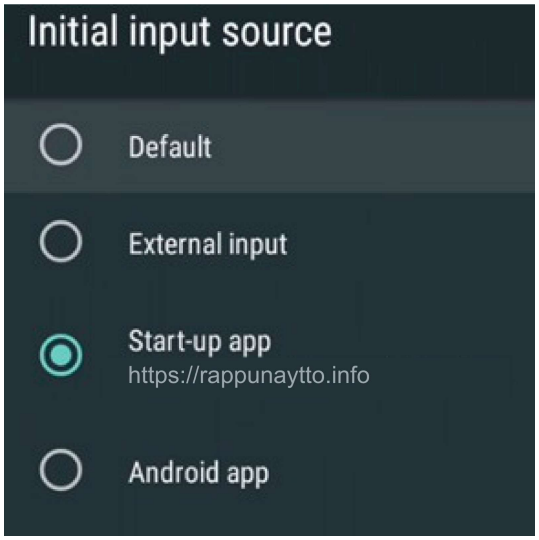
Kuva 15. Pro mode-lukitus.



Kuva 16. PIN-koodin määritys.

4.3.1 Oletustulolähde

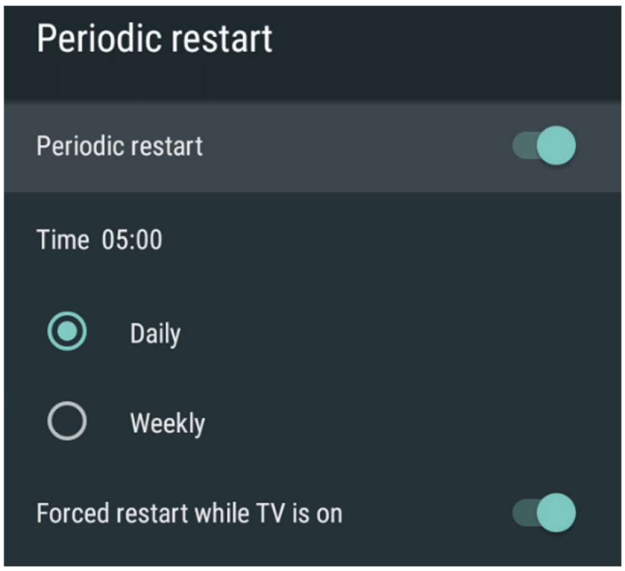
TV:ssä tullaan näyttämään taloyhtiön tietoja. Tähän tarkoitukseen on luotu oma sovellus, joka näyttää taloyhtiön rapputiedot, tärkeimmät yhteystiedot sekä uusimmat tiedotteet. Sovellusta voi käyttää Androidille asennettavalla sovelluksella tai selaimen kautta verkko-osoitteessa. Aikaisemmin sovelluksen ja Android tv:n kanssa olleiden haasteiden vuoksi valittiin verkko-osoitteen käyttäminen paremmaksi vaihtoehdoksi. Kuvassa 17 verkko-osoite määritetään pro mode-asetuksien kautta oletussovellukseksi, joka avataan aina uudelleenkäynnistymisen yhteydessä.



Kuva 17. Oletussovelluksen määrittäminen.

4.3.2 Käynnistyminen

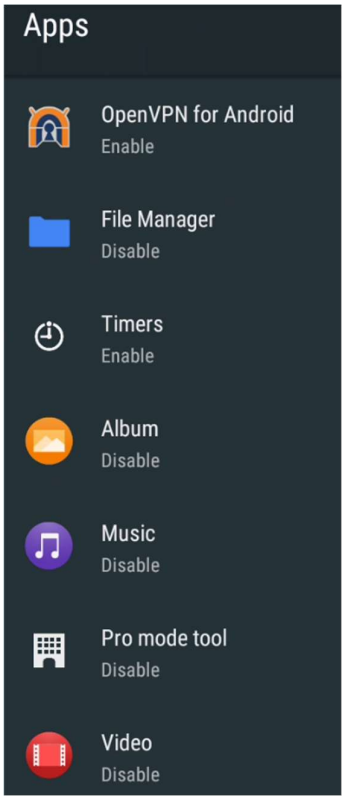
TV:n toimivuuden varmistamiseksi sekä mahdollisten virhetilanteiden minimoimiseksi on tv määritetty käynnistymään jokaisena aamu kello 5.00.



Kuva 18. Uudelleenkäynnistyminen pakotetusti.

Uudelleenkäynnistyminen pakotetaan tehtäväksi tv:n ollessa päällä ja vaikka tv olisi sammutettu (lepotilassa), käynnistyy se uudelleen esiasetetun ajan mukaisesti. Kuvassa 18 uudelleenkäynnistymisen määrittäminen.

Toisinaan on törmätty tilanteeseen, jossa internetyhteys on hetkellisesti kadotettu, eikä tv ole sen jälkeen kyennyt lataamaan sivua uudestaan. Uudelleenkäynnistämisellä pakotetaan toimintojen käynnistyminen uudelleen.



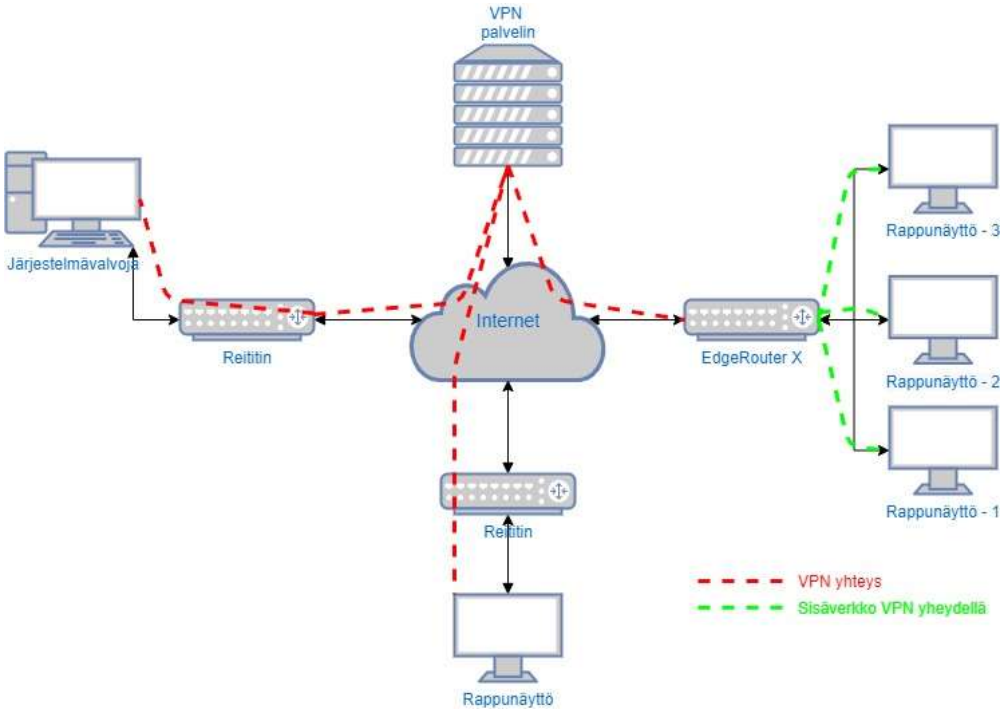
Kuva 19. Sovellukset.

Sovelluksista ainoastaan OpenVPN ja Timers on sallittu kuvassa 19. OpenVPN sovelluksen avulla tv ottaa yhteyden VPN serverille. OpenVPN sovellukseen kopioidaan VPN-palvelimella luotu .ovpn-tiedosto, jonka avulla etähallittava laite ottaa

VPN-yhteyden palvelimelle. Sovelluksessa määritettään haluttu ovpn-profiili oletukseksi ja asetetaan yhteys käynnistymään automaattisesti uudelleenkäynnistyksen yhteydessä.

4.4 VPN-yhteys

Tutkimustyön aikana tutkittiin erilaisia mahdollisuuksia toteuttaa VPN-palvelin, johon kaikki laitteet ottavat yhteyden. VPN yhteyden avulla voidaan yhdistää eri verkoissa olevia laitteita samaan verkkoon. Yhteys luo ”tunnelin” laitteiden välille. Tunnelin avulla data pysyy turvassa ja minimoi ulkopuolisten henkilöiden pääsemisen käsiksi dataan. Kuvassa 20 on diagrammin, miten yhteys tullaan muodostamaan palvelimen ja laitteiden välillä.



Kuva 20. VPN-diagrammi yhteyden muodostuksesta.

4.4.1 VPN-palvelin

VPN-sovelluksena on käytetty GitHubista käyttäjän Angristan tekemää asennusskriptiä openvpn-install (Stanislas Angristan, OpenVPN-install). Asennusskriptin avulla saadaan perusasetukset VPN-palvelimelle ja sitä käytetään myös uusien asiakkaiden lisäämiseen.

Yrityksen VPN-palvelin asennettiin OVH:n Virtual Private-serverille. VPS-palvelimelle asennettu virtuaalikone käyttää Centos 7 Linux pohjaista käyttöjärjestelmää. Graafista käyttöliittymää ei palvelimelle asennettu vaan asennukset tehtiin käyttämällä SSH-yhteyttä ja OVH cloudin tarjoamaa KVM-konsolia.

Toinen vaihtoehto olisi käyttää omalle palvelimelle asennettuna OpenVPN Access Serveriä. Tässä toteutustavassa laitteiden hallinta olisi helpompaa Access serverin oman hallintasivun kautta. Asetuksia pystyy määrittämään nopeasti ja helposti. Kustannussyistä tämä vaihtoehto jätettiin pois toistaiseksi.

4.4.2 VPS-palvelimen turvallisuus

Virtuaalitietokone on OVH:n ylläpitämällä palvelimella. Käyttöjärjestelmä valittiin yhdenmukaisuussyistä Centos 7. Yrityksen muut palvelimet ovat myös Centos 7 käyttöjärjestelmällä ylläpidettyjä ympäristöjä.

Palvelimen turvallisuuteen liittyvissä asioissa huomioitiin etäyhteyden ottaminen. Ominaisuudet, joille ei ollut käyttöä, pyrittiin ottamaan pois käytöstä. Root käyttäjän kirjautuminen estettiin SSH-yhteyden kautta muokkaamalla tiedostoa ”/etc/ssh/sshd_config”. SSH-asetuksiin määritettiin myös tietyt IP-osoitteet, joita SSH kuuntelee. Vain näiden osoitteiden kautta pystytään kirjautumaan palvelimelle SSH:ta käyttäen.

Käyttäjätunnus- ja salasanayhdistelmä on haavoittuvainen tapa kirjautua. Päädyimme käyttämään SSH-yhteyttä avainpareilla. Avainpari on hieman turvalli-

sempi vaihtoehto verrattuna perinteiseen käyttäjätunnus- ja salasanayhdistelmään. Tässä tavassa palvelimelle kopioidaan yhteyslaitteelta avainparin julkinen avain. Tämä mahdollistaa kirjautumisen ilman salasanaa eikä sitä näin ollen tarvitse tallentaa tiedostoihin.

Mikäli avainpari on määritetty salasanaa käyttämällä, täytyy yhteyden muodostamisen yhteydessä syöttää avainparin salasana. Salasanallinen kirjautuminen avainparin kanssa on näistä vaihtoehdoista paras mahdollinen tapa. SSH-asetuksista poistimme tämän jälkeen mahdollisuuden kirjautua salasana-käyttäjänimiyhdistelmällä.

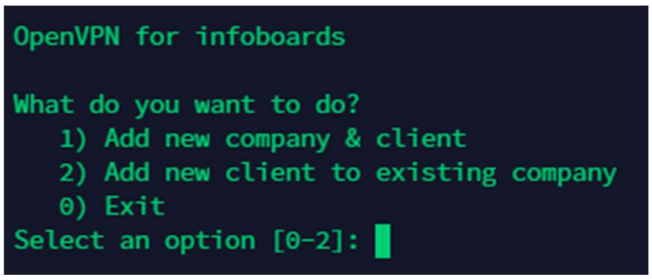
4.4.3 VPN-palvelimen käyttö

GitHubin kautta ladattu ja asennettu skripti toimi osittain halutulla tavalla. Laitteiden ottaessa yhteyden palvelimeen saavat ne IP-osoitteen samasta verkon osoiteavaruudesta. Palomuuriasetuksilla voidaan estää muiden laitteiden näkyminen toisille laitteille, mutta joissakin käyttökohteissa saattaa olla useita laitteita ja nämä laitteet saisivat näkyä samassa verkkoalueessa. Tästä syystä päädyttiin tekemään toinen skripti, jonka avulla saadaan tehtyä jokaiselle asiakkaalle oma verkon osoitealue. Laitteita voi myöhemmin lisätä olemassa olevaan alueeseen uutta asiakasta lisätessä, uusi skripti kutsuu alkuperäistä openvpn-install skriptiä.

4.4.4 Asiakkaan lisääminen

Uutta asiakasta lisättäessä on otettava SSH-yhteys VPN-palvelimeen. Alkuperäisessä skriptissä, kuvassa 21, käyttäjältä kysytään uuden asiakkaan nimi sekä kirjautumistapa. Kirjautumistapa voi olla ilman salasanaa tai salasanan kanssa. Toteutuksessa valittiin salasanaton kirjautumistapa.

Kuva 21. Asiakkaan lisääminen alkuperäinen skripti (Stanislas Angristan, OpenVPN-install).



Kuva 22. Skriptin aloitusvalikko.

Uudessa skriptissä, kuvassa 22, käyttäjältä kysytään aluksi, halutaanko lisätä uusi yritys ja asiakas (1) vai lisätäänkö asiakas olemassa olevaan yritykseen (2). Valinnasta riippuen, ohjelma suorittaa komennot halutulla tavalla.

```
function newCompany() {
    echo ""
    echo "Enter new company VAT-number (Y-TUNNUS)"
    until [[ $C_COMPANY =~ ^[a-zA-Z0-9_-]+$ ]]; do
        read -rp "VAT-number: " -e C_COMPANY
    done
    echo "Enter name of company"
    until [[ $C_COMPANY_NAME =~ ^[a-zA-Z0-9_-]+$ ]]; do
        read -rp "Name: " -e C_COMPANY_NAME
    done
    echo "Enter new client (NUMBER+STAIRWAY). Prefix is "$C_COMPANY"_"
    until [[ $C_CLIENT =~ ^[a-zA-Z0-9_-]+$ ]]; do
        read -rp "Client: "$C_COMPANY"_" -e C_CLIENT
    done

    openVPNscript
}
```

Kuva 23. Skripti – uusi yritys ja asiakas.

```
Select an option [0-2]: 1

Enter new company VAT-number (Y-TUNNUS)
VAT-number: 98765432
Enter name of company
Name: testi_oy

Enter new client (NUMBER+STAIRWAY). Prefix is 98765432_
Client: 98765432_1A
```

Kuva 24. Uusi yritys ja asiakas.

Kuvassa 24 lisätään uusi yritys ja asiakas. Ohjelma kysyy yrityksen y-tunnuksen, nimen sekä käyttäjän nimen. Käyttäjännimessä käytetään yrityksen y-tunnusta alkuosana. Nimen alkuosa helpottaa mahdollisien ongelmatilanteiden selvittämistä, kun esimerkiksi pitää tarkistaa milloin laite on viimeksi ollut yhteydessä palvelimeen. Kuvassa 23 on osa uutta skriptiä, joka suoritetaan kuvassa 24. Kysytyt arvot tallennetaan muuttujiin, joita käytettään skriptin muissakin vaiheissa.

```
Select an option [0-2]: 2

Enter company id VAT-number where you want to add client
VAT-number: 98765432

The specified company was found 98765432

Enter new client (NUMBER+STAIRWAY). Prefix is 98765432_
Client: 98765432_1B
```

Kuva 25. Uusi käyttäjä olemassa olevaan yritykseen.

```
echo "Enter company id VAT-number where you want to add client"
until [[ $C_COMPANY =~ ^[a-zA-Z0-9_-]+$ ]]; do
    read -rp "VAT-number: " -e C_COMPANY
done

CLIENTEXISTS=$(tail -n +2 /etc/openvpn/script/vpn.txt | grep -c -E "$C_COMPANY")
if [[ $CLIENTEXISTS == '1' ]]; then
    echo ""
    echo "The specified company was found "$C_COMPANY""
    echo ""
    echo "Enter new client (NUMBER+STAIRWAY). Prefix is "$C_COMPANY"_"
    until [[ $C_CLIENT =~ ^[a-zA-Z0-9_-]+$ ]]; do
        read -rp "Client: "$C_COMPANY"_" -e C_CLIENT
    done
```

Kuva 26. Skripti – uusi käyttäjä olemassa olevaan yritykseen.

Kuvassa 25 lisätään uusi käyttäjä olemassa olevaan yritykseen. Ohjelma kysyy käyttäjältä yrityksen y-tunnuksen ja tarkistaa löytyykö y-tunnusta jo järjestelmästä. Mikäli yritys löytyy järjestelmästä, pyydetään käyttäjää syöttämään käyttäjänimi uudelle asiakkaalle. Kuvassa 26 on skriptin osa missä tarkistetaan, onko syötetty y-tunnus jo järjestelmässä. Yrityksen tiedot tallennetaan tekstitiedostoon luomisvaiheessa. Tätä tiedostoa luetaan, kun lisätään asiakasta olemassa olevaan yritykseen.

```
Select an option [0-2]: 2

Enter company id VAT-number where you want to add client
VAT-number: 12345678

Entered company was not found. Do you wan't to add new company?
Yes or No [y,n]
```

Kuva 27. Yritystä ei löydy.

Mikäli syötettyä y-tunnusta ei löydy järjestelmästä, ilmoittaa ohjelma siitä ja antaa vaihtoehdon syöttää uusi yritys järjestelmään vahvistamalla valinta kuvassa 27. Vahvistuksen jälkeen toimitaan kuvan 25 mukaisesti.

Edellä mainittujen tapojen 1 tai 2 mukaisen toiminnan jälkeen skripti kutsuu alkuperäistä skriptiä, joka suorittaa tarpeelliset asiat OpenVPN:n liittyen. Skriptiä kutsutaan lisäparametrien avulla, jolloin tietoja ei tarvitse syöttää uudestaan. Parametrit ovat 1. uusi asiakas, 2. asiakkaan nimi (y-tunnus ja asiakas), 3. salasanaton kirjautuminen. Kuvassa 28 osa skriptiä missä kutsutaan alkuperäistä skriptiä (Stanislas Angristan, OpenVPN script with export).

```
function openVPNscript() {
    #Run openvpn script to create new user
    export MENU_OPTION="1"
    export CLIENT=$C_COMPANY"_"$C_CLIENT
    export PASS="1"

    /home/centos/openvpn/openvpn-install.sh
}
```

Kuva 28. Alkuperäisen skriptin kutsuminen uuden skriptin kautta.

4.4.5 Laitteen yhdistäminen

Laitteen yhdistäminen VPN-palvelimeen tapahtuu käyttämällä OpenVPN Connect-sovellusta yhdessä ovpn-tiedoston kanssa. Ovpn-tiedosto luodaan, kun uusi asiakas lisätään järjestelmään. Tiedoston lataamisen helpottamiseksi päädyttiin kopioimaan tiedostot yrityksen Google Drive-pilvipalveluun. Tiedoston siirtäminen tapahtuu automaattisesti samalla, kun uutta asiakasta lisätään järjestelmään. Tiedostojen kopioimiseen Google Driveen käytetään rclone-ohjelmaa. Kuvassa 29 osa skriptiä, joka siirtää ovpn-tiedoston olemassa olevaan yrityksen kansioon tai luo yritykselle uuden kansion, mikäli sitä ei vielä ole. Lopuksi tiedostot synkronoidaan Google Driveen.

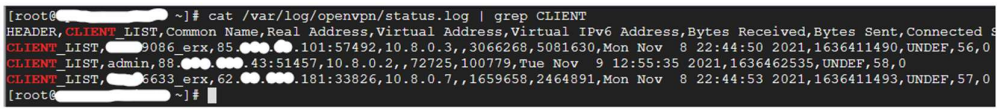
```
function ovpn() {
    #Move ovpn file to client folder of openvpn and copy files to Google Drive

    if [[ -d /etc/openvpn/client/$C_COMPANY ]]; then

        mv $CLIENT.ovpn /etc/openvpn/client/$C_COMPANY
        #Copy ovpn files to the GoogleDrive for easier access
        /home/centos/Drive/drive.sh
        exit 0
    else
        #Create new folder for client if not found
        mkdir /etc/openvpn/client/$C_COMPANY
        mv $CLIENT.ovpn /etc/openvpn/client/$C_COMPANY
    fi

    #Copy ovpn files to the GoogleDrive for easier access
    /home/centos/Drive/drive.sh
}
```

Kuva 29. Skripti – tiedostojen siirtäminen.

Rclone-ohjelmalla määritetään uusi yhteys palvelimen ja Google Driven välille. Yhteyden muodostamista varten määritetään Google Drive API key. APIin avulla voidaan muodostaa yhteys palvelun ja tietokoneen välillä. Google Drive API määritettiin käyttöön kirjautumalla Google Cloud Platform-työkaluun ja luomalla uusi projekti. (Google, Google Cloud Platform) Projektiin lisätään Google Drive API (Google, Google Drive API). Määrityksien jälkeen palvelusta kopioidaan Client ID ja Client Secret, joita tarvitaan yhteyden muodostamiseen Rclonen ja Google Driven yhteyden muodostamiseen (Rclone, Rclone config).

5 RAPPUNÄYTÖN TILAKYSELYIDEN TEKEMINEN

VPN-yhteydellä yhdistettyjen laitteiden tilaa voidaan kysyä kahdella eri tavalla. Yhdistetyt laitteet voi tarkistaa VPN-palvelimen komentokehotteesta. Palvelimelle tulee ottaa SSH-yhteys määritetyllä tavalla. OpenVPN-palvelulla on oma loki tiedostonsa mihin tiedot kirjataan, kun muutoksia tulee. Kuvassa 30 on lokitiedoston tuloste.



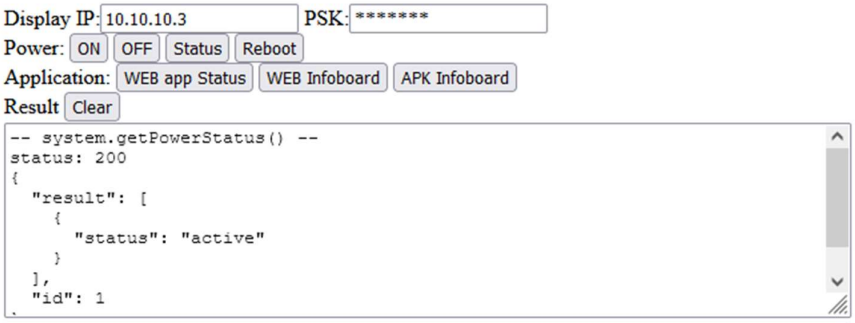
Kuva 30. VPN-yhdistetyt laitteet.

Kuvan 30 tulosteessa on peitetty asiakkaiden y-tunnuksen alkuosa sekä julkisen IP-osoitteen keskiosa. Lisäksi VPN-palvelimen nimi/osoite on peitetty. Lokitiedostossa kiinnostavimmat asiat ovat:

- Asiakkaan nimi
- Julkinen IP-osoite
- VPN-verkon IP-osoite
- Yhteyden muodostamisen aloitusajankohta

Kuvassa 30 näkyy kolme VPN-yhteyttä. Kaksi yhteyttä on otettu EdgeRouterin kautta ja kolmas yhteys on järjestelmänvalvojan tietokoneelta otettu yhteys. Reitittimen takana omassa sisäverkossa on rapputaulut. Rapputaulujen tilatietojen kyselyä varten pitää tietää sisäverkon osoitteet. Jokaisen rapputaulun tiedot on dokumentoitu turvalliseen paikkaan, mistä voidaan tarpeen vaatiessa tiedot lukea.

Sony-televisioita varten on olemassa oma HTML pohjainen sivu, jota voi hyödyntää tilakyselyiden suorittamiseen. Esimerkkitiedoston voi ladata Sonyn sivujen kautta (Sony, Samples REST API HTML). Tilatietoja voi kysyä VPN yhteyden ollessa aktiivinen järjestelmänvalvojan tunnuksella.



Kuva 31. HTML Sony REST API-hallintasivu.

Kuvassa 31 on muokattu Sonyn HTML esimerkkiä niin, että tarpeelliset toiminnot ovat saatavilla. Ylimmällä rivillä tulee syöttää laitteen sisäverkon IP-osoite tai VPN IP-osoite, mikäli kohteessa on vain yksi näyttö tai se on yhdistetty suoraan VPN-palvelimeen. Lisäksi rappunäyttöön aikaisemmin määritelty ”pre-shared-key” syötetään PSK kohtaan. Laitteen ”Status” eli tilatiedon voi kysyä ilman salasanan syöttämistä. Muihin toimintoihin salasana on vaadittu. Toimintojen ja komentojen tarkempi dokumentaatio löytyy Sonyn sivuilta (Sony, REST API Dokumentaatio).

- Power
    - ON – Komento käynnistää näytön
    - OFF – Komento sammuttaa näytön
    - Reboot – Komento käynnistää laitteen uudestaan
    - Status – Komento tulostaa laitteen tilan.
- Application
    - WEB app Status – Komento tulostaa verkkoselaimen tilan.
        - Aktiivinen – ”Totta / epätosi”
        - URL – verkko-osoite
    - WEB infoboard
        - Lähettää komennon avata verkkoselain rappunäytön verkko-osoitteeseen
    - APK infoboard
        - Lähettää komennon avata rappunäyttösovellus

6 YHTEENVETO JA TULEVAISUUDEN SUUNNITELMIA

Opinnäytetyön aikana toteutettu etähallinta saatiin toteutettua osittain halutulla tavalla. Käytössä olleet laiteet ja niiden erilaiset käyttöliittymät pakottivat kahden erilaisen järjestelmän toteuttamiseen. Sonyn valmistamaan laitteeseen löydettiin toimiva ratkaisu hyödyntäen laitteen omaa ohjelmistoa, eikä erillistä hallintaohjelmistoa tarvittu. Yhteyden muodostaminen laitteeseen jouduttiin rakentamaan VPN yhteydellä, jota varten täytyi oma palvelin hankkia.

Yrityksen toinen laite, 24 tuumainen kosketuksellinen Android rappunäyttö vaati erilaisen ratkaisun. Tämän laitteen kanssa päädyttiin käyttämään ulkopuolisen palveluntarjoajan maksullista MDM-ohjelmistoa. Ohjelmisto mahdollistaa selainpohjaisen keskitetyn laitehallinnan. Laitteiden asetuksia voidaan muokata selaimen kautta ja myös asentaa rappunäyttösovelluksen päivityksiä.

Kahden erilaisen järjestelmän ylläpitäminen rappunäyttöjen hallintaan ei ole pidemmällä aikavälillä tehokasta. Manuaalisten tarkistuksien tekeminen vie järjestelmänvalvojalta paljon työaikaa, kun pitää suorittaa monia eri vaiheita. Olisikin kannattavaa hyödyntää rajapintojen tuomia mahdollisuuksia ja rakentaa tuotanto palvelimen BackOfficeen hallintapaneeli rappunäytöille. Rappunäyttöjen tarpeellinen tieto tuotaisiin yhteen hallintanäkymään mistä järjestelmänvalvoja voi hallita yksittäistä näyttöä tarpeen vaatiessa. Automatisoitujen prosessien suorittaminen olisi myös mahdollista toteuttaa rajapintojen avulla. Mikäli rappunäytön tilatiedot eivät vastaa kriteereitä, voitaisiin sinne lähettää komennot, joilla saadaan tilatiedot vastaamaan haluttuja kriteereitä.

Opinnäytetyö oli mielenkiintoinen prosessi minkä aikana oppi paljon erilaisia asioita laitteiden hallinnasta virtuaalisen palvelimen pystyttämiseen ja hallintaan. Projektin aikana tuli huomattua kuinka tärkeää jokaisen suoritetun työvaiheen dokumentointi on. Testien suorittamista varten on monta kertaa pitänyt aloittaa alusta, jotta on voinut löytää parhaimman ja tehokkaimman tavan suorittaa erilaiset työvaiheet.

LÄHTEET

Sand Studio, Airdroid about. Viitattu 7.11.2021 https://www.air-droid.com/en/about-us/

Sand Studio, Airdroid Security. Viitattu 11.11.2021 https://www.air-droid.com/en/resources/security/

Zoho Corporation, ManageEngine about-us. Viitattu 11.11.2021 https://www.manageengine.com/company.html?MEfooter

Zoho Corporation, ManageEngine Security. Viitattu 10.11.2021 https://www.manageengine.com/security.html?MEfooter

Zoho Corporation, ManageEngine Device Owner. Viitattu 11.11.2021 https://www.manageengine.com/mobile-device-manage-ment/help/android_for_work/mdm_device_owner_provisioning_adb.html

Mitsogo Inc, Hexnode about-us. Viitattu 10.11.2021 https://www.hexnode.com/about-us/

Mitsogo Inc, Hexnode Architecture. Viitattu 10.11.2021 https://cdn.hexnode.com/mobile-device-management/help/wp-content/up-loads/2020/09/05091300/Hexnode-architecture-scaled.jpg

Mitsogo Inc, Hexnode security. Viitattu 10.11.2021 https://www.hexnode.com/mobile-device-management/help/hexnode-cloud-infrastructure-security/

Ubiquiti, EdgeRouter X L2TP. Viitattu 7.11.2021 https://help.ui.com/hc/en-us/ar-ticles/204950294

Ryan Scullen, 2017 EdgeRouter X OpenVPN. Viitattu 8.11.2021 https://ryanscul-len.wordpress.com/2017/07/24/openvpn-client-setup-on-edgeos/

Stanislas Angristan, OpenVPN-install. Viitattu 29.7.2021 https://github.com/Ang-ristan/OpenVPN-install

Stanislas Angristan, OpenVPN script with export. Viitattu 8.11.2011 https://git-hub.com/angristan/openvpn-install/issues/821

Google, Google Cloud Platform. Viitattu 8.11.2021 https://develo-pers.google.com/workspace/guides/create-project

Google, Google Drive API. Viitattu 8.11.2021 https://develop-ers.google.com/drive/api/v3/enable-drive-api

Rclone, Rclone config. Viitattu 8.11.2021 https://rclone.org/drive/

Sony, Samples REST API HTML. Viitattu 8.11.2021 https://pro-bravia.sony.net/develop/integrate/ip-control/samples/index.html

Sony, REST API Dokumentaatio. Viitattu 9.11.2021 https://pro-bravia.sony.net/develop/integrate/rest-api/spec/