

Janne Raappana

## **MOBIILITUNNISTESOVELLUS KULUNVALVONTAAN**

# **MOBIILITUNNISTESOVELLUS KULUNVALVONTAAN**

Janne Raappana  
Opinnäytetyö  
Syksy 2021  
Tietotekniikan tutkinto-ohjelma  
Oulun ammattikorkeakoulu

## TIIVISTELMÄ

Oulun ammattikorkeakoulu  
Tietotekniikan tutkinto-ohjelma, ohjelmistokehitys

---

Tekijä: Janne Raappana

Opinnäytetyön nimi: Mobiilitunnistesovellus kulunvalvontaan

Työn ohjaajat: Pertti Heikkilä, Eino Niemi

Työn valmistumislukukausi ja -vuosi: Syksy 2021

Sivumäärä: 45 + 6

---

Älypuhelimet ovat päivä päivältä yhä isompi osa meidän jokapäiväistä arkeamme. Tämän opinnäytetyön lähtökohtana oli toteuttaa Idesco Oy:lle uusi mobiilitunnistetta hyödyntävä ratkaisu kulunvalvontaan. Tarkoituksena oli luoda mahdollisimman käyttäjäystävällinen ratkaisu mobiilitunnisteen käyttöönottamiseen kulunvalvonnassa.

Työ aloitettiin suunnittelemalla mahdollista ratkaisua ja esitutkimalla markkinoilla olevia ratkaisuja. Mobiilisovelluksen käyttöympäristöksi päädyttiin ottamaan Microsoftin Visual Studiossa oleva mobiilikehitysympäristö Xamarin. Xamarinissa käytetään korkean tason ohjelmointikieltä C#:a ja projektin pääkehityskohteena on älypuhelimien Android-käyttöjärjestelmä. Laajentaminen iOS-käyttöjärjestelmään oli myös tarkoituksena myöhemmin, mikä on myös hyvin mahdollista Xamarin-kehitysympäristöllä. Ratkaisussa käytetään Bluetooth Low Energy -tekniikkaa kulunvalvontalukijoiden ja mobiilisovelluksen välisessä kommunikoinnissa. Lopuksi luotu mobiilisovellus toteutettiin kommunikoimaan Idesco Oy:n lukijoiden kanssa. Lukijoiden laiteohjelman muutokset eivät kuuluneet opinnäytetyöhön. Projektin toteutukseen käytettiin Idescon sisäistä prosessimallia ja omatoimisen kehitysaikaisen testauksen lisäksi väliversioita testasivat Idescon testaajat.

Projektissa onnistuttiin hyvin. Menetelmät työn toteutukseen osoittautuivat hyödyllisiksi kehitysaikana sekä myös tulevaisuudessa. Valmis sovellus on helppokäyttöinen ja hyödyllinen kokonaisuus, jonka avulla Idesco Oy:n kulunvalvontaa saatiin laajennettua käyttämään myös älypuhelimia etätunnistimena ilman internet-yhteyttä. Projektin vapaa vastuullisuus ja aikaisemmat vapaa-ajan harrastukset mahdollistivat luovuuden suunnittelussa, toteutumisessa ja onnistumisessa. Tuote päätyi myöhemmin asiakkaille asti ja projekti herätti jo ennalta suurta kiinnostusta Idesco Oy:n asiakkaisissa.

---

Asiasanat: Kulunvalvonta, etätunnistus, tunnistimet, Bluetooth, langaton tekniikka, mobiiliohjelmointi, mobiilisovellukset

## ABSTRACT

Oulu University of Applied Sciences  
Degree Programme in Information Technology, Software Development

---

Author: Janne Raappana

Title of thesis: Mobile ID Application to Access Control

Supervisors: Pertti Heikkilä, Eino Niemi

Term and year when the thesis was submitted: Autumn 2021    Number of pages: 45 + 6

---

Smartphones are getting bigger part of our everyday lives. The starting point for this thesis was to implement new solution for access control system to utilize smartphones. Purpose was to create a mobile ID solution that is the most user friendly as possible.

The project got started by planning the best possible solution and doing research of the possible solutions already in the market. For application implementation, the integrated development environment was chosen to be Xamarin in Microsoft's Visual Studio. Xamarin is cross-platform mobile development environment. Xamarin uses high level programming language C#, and the project was aimed forward Android mobile operating system. There was also a plan to extend the project to also include iOS mobile operating system after the thesis. For the communication, the solution uses Bluetooth Low Energy -technology to communicate between the smartphone and the access control reader. In the end, the smartphone application was implemented to communicate with Idesco Oy's access control readers. Programming of the access control reader was not part of the thesis. Idesco Oy's internal process model was used for the implementation process and for the other than self-employed testing during the development, the Idesco Oy's testers were employed.

The project ended well. The methods used for the development were useful during the development and in the future. The final mobile application is user-friendly and useful solution which was able to extend the Idesco Oy's product portfolio to include Mobile ID solution without an external database or a cloud. The freedom of choice during the project and friendly atmosphere at the workplace made it possible to have creative mind for the planning, development and for the success of the project. Later, the final product was given to customers and beforehand the project caused a lot of excitement aimed forwards Idesco Oy.

---

Keywords: Access control, remote authentication, transponders, Bluetooth, wireless technology, mobile programming, mobile applications

## ALKULAUSE

Tämä opinnäytetyö on tehty vuosien 2019–2021 aikana Idesco Oy:lle. Projekti aloitettiin kesällä 2019 ja toteutus valmistui 2019 syksyn aikana. Tehtävänä oli toteuttaa käyttäjäystävällinen ratkaisu mobiilitunnisteen käyttöönottoon kulunvalvonnassa. Haluan kiittää Idescoa hyvästä opinnäytetyöaiheesta. Kiitos myös Paula Koistiselle projektin sulautetun puolen toteutuksesta sekä neuvoista. Esimiehille Juha Polvelalle ja Jaana Ojalalle sekä työn valvojille Pertti Heikkilälle ja Eino Niemelle haluan antaa kiitokset opinnäytetyöni ohjauksesta. Kiitos kaikille Idescolaisille projektiin osallistumisesta ja hyvästä yhteishengestä!

Oulussa 21.10.2021

Janne Raappana

# SISÄLLYS

TIIVISTELMÄ

ABSTRACT

SISÄLLYS

ALKULAUSE.....	5
SANASTO.....	8
1 JOHDANTO .....	10
2 KULUNVALVONTAJÄRJESTELMÄT .....	11
2.1 Kulunvalvontajärjestelmä yleisesti.....	11
2.2 Tunnistusmenetelmiä .....	12
2.2.1 PIN-koodi .....	12
2.2.2 Etätunnistin .....	12
2.2.3 Biometriset tunnisteet .....	13
2.2.3.1 Sormenjälki.....	14
2.2.3.2 Kasvot.....	15
2.2.3.3 Silmä.....	16
2.2.4 Mobiilitunnistin .....	16
2.2.5 Mahdolliset tulevaisuuden tunnistimet.....	17
2.3 Pohdinta tunnistusmenetelmistä.....	17
3 PUHELIMESTA LÖYTYVÄT TUNNISTEET .....	19
3.1 Secure Android ID .....	19
3.2 UUID .....	20
3.3 IMEI, MEID, ESN, IMSI .....	20
3.4 MAC- ja Bluetooth-osoite.....	20
3.5 Sarjanumero.....	20
3.6 Advertising ID .....	21
3.7 Instance ID .....	21
3.8 Tunnisteiden pohdinta .....	21
4 MOBIILIRATKAISUT MARKKINOILLA .....	23
4.1 HID .....	23
4.2 Bitwards.....	24
4.3 Lenel .....	25

4.4	STid .....	25
4.5	Nedap .....	26
4.6	AMAG .....	27
4.7	Mobiiliratkaisujen pohdinta .....	28
5	TOTEUTUS .....	29
5.1	Lähtötilanne .....	29
5.2	Vaatimusmäärittely .....	29
5.3	Esiselvitys .....	30
5.4	Ratkaisun suunnittelu .....	30
5.5	Käyttöliittymä .....	32
5.6	Kommunikointi .....	33
5.7	Salaus .....	34
5.8	Kehitysympäristö .....	34
5.9	Käytettyjä tekniikoita .....	36
5.9.1	DependencyService .....	36
5.9.2	MessagingCenter .....	36
5.9.3	Foreground service .....	37
6	POHDINTA .....	38
	LÄHTEET .....	40
	LIITTEET .....	46

## SANASTO

AES	Advanced Encryption Standard eli lohkosalausmenetelmä
Android	Avoimen lähdekoodin mobiilikäyttöjärjestelmä, joka on Googlen sponsoroima
BLE	Bluetooth Low Energy eli pienen virran langaton yhteysteknologia
DNA	Deoksiribonukleiinihappo eli nukleiinihappo, joka sisältää eliöiden geneettisen materiaalin
Duplikaatti	Identtinen esine
ESN	Equipment Serial Number eli valmistajan luoma laitteen yksilöllinen tunniste
GATT	Generic Attribute Profile eli profiili, joka määrittää miten kaksi BLE-laitetta kommunikoivat keskenään
GPS	Global Positionin System eli maailmanlaajuinen satelliittipaikannusjärjestelmä
ID	Identifier eli tunniste
IMEI	International Mobile Equipment Identity eli tehdasasennettu yksilöllinen sarjanumero
IMSI	International Mobile Subscriber Identity eli puhelimen SIM-kortille tallennettu numerosarja
iOS	Applen luoma ja kehittämä mobiilikäyttöjärjestelmä
Kryptaus	Kryptologian prosessi, jossa viesti piilotetaan niin, että vain tietyt osapuolet voivat lukea sitä



MAC	Media Access Control, yksilöllinen tunniste Internet-kommunikoinnissa
MEID	Mobile Equipment Identifier on tehdasasennettu yksilöllinen sarjanumero, joka on sama kuin IMEI, mutta yhden numeron lyhyempi
NFC	Near-field Communication eli RFID-tekniikkaa hyödyntävä tiedonsiirtomenetelmä
PIN	Personal Identification Number, tunnusluku
Reset	Prosessi, joka palauttaa laitteen normaaliin tilaansa
RFID	Radio Frequency Identification eli radiotaajuinen etätunnistus
Root	Unix-järjestelmissä root- eli pääkäyttäjä, jolla on oikeus muuttaa kaikkia laitteen tietoja
SIM	Subscriber Identity Module eli älykortti, jossa on yksilöllinen matkapuhelinliittymän avain
UUID	Universally Unique Identifier, yleisesti yksilöllinen tunniste
Wi-Fi	Langaton lähiverkko, tunnetaan myös nimellä WLAN

# 1 JOHDANTO

Älypuhelimista on tullut osa meidän jokapäiväistä arkea. Nyky-yhteiskunta suosii laitteita ja ratkaisuja, jotka tekevät arkielämästämme helppoa ja mukavaa. (1.) Tämän opinnäytetyön lähtökohtana oli toteuttaa Idesco Oy:lle uusi mobiilitunnistetta hyödyntävä ratkaisu kulunvalvontaan.

Idesco Oy on vuonna 1989 perustettu oululainen RFID-laitteita ja -tunnisteita valmistava kulunvalvontaan erikoistunut teknologiayritys. Älypuhelimien yleistymisen myötä Idesco Oy on halunnut laajentaa kulunvalvontavalikoimansa käyttämään myös nykyaikaisia mobiilitunnisteita. Projektin tarkoituksena oli luoda kevyt ratkaisu mobiilitunnisteen käyttöönottamiseen kulunvalvonnassa mobiilisovelluksen muodossa.

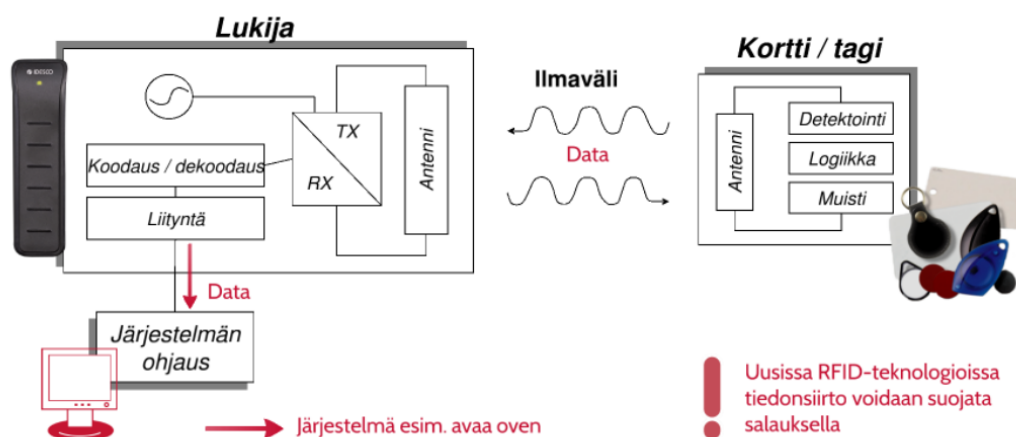
Toteutuksen suhteen käyttöympäristöksi päädyttiin ottamaan Microsoftin Visual Studiossa oleva mobiilikehitysympäristö Xamarin. Xamarinissa käytetään korkean tason ohjelmointikieltä C#:a ja projektin pääkohteena on älypuhelimien Android-käyttöjärjestelmä. Ratkaisussa käytetään Bluetooth Low Energy -tekniikkaa lukijoiden ja mobiilisovelluksen välisessä kommunikoinnissa. Luodun sovelluksen nimeksi päädyttiin antamaan Idesco Mobile Lite ja mobiilisovellus toteutettiin kommunikoimaan Idesco Oy:n kulunvalvontalukijoiden kanssa.

## 2 KULUNVALVONTAJÄRJESTELMÄT

### 2.1 Kulunvalvontajärjestelmä yleisesti

Kulunvalvonta on alueella, rakennuksessa tai muualla liikkuvien henkilöiden valvontaa vartiointilla tai teknisillä laitteilla (2). Kulunvalvonnan päätarkoituksena on estää halutulla alueella kulkeminen asiattomilta henkilöiltä (3).

Jotta henkilön kulkemista voidaan hallita kulunvalvonnassa, on hänet ensin tunnistettava. Sähköisissä kulunvalvontajärjestelmissä tunnistusmenetelmänä voidaan käyttää erilaisia tunnistimia tai tunnuskoodia, joiden tunnistamiseen käytetään kulunvalvontalukijoita. (3.) Kulunvalvontalukija yhdistetään oven sähkölukkoon ja kulunvalvontajärjestelmään, josta voidaan helposti hallita henkilön kulkuoikeuksia alueella. Kulunvalvontalukijat ovat yhteyksissä järjestelmään erilaisilla tiedonsiirtoprotokollilla, mutta tässä työssä keskitytään enimmäkseen tunnistusmenetelmiin ja niiden kehittämiseen. RFID-tunnistamisen toimintaperiaate näkyy kuvassa 1.



KUVA 1. RFID-tunnistamisen toimintaperiaate (4)

## 2.2 Tunnistusmenetelmiä

### 2.2.1 PIN-koodi

PIN-koodi on käyttäjän muistitietoon perustuva tunnistusmenetelmä ja se on yleisesti käytössä kulunvalvonnassa. PIN-koodin käyttötapana yleensä on olla vara- tai lisävaihtoehtona lukijoissa etätunnistimen rinnalla. PIN-koodin heikkous on kuitenkin sen unohdettavuus ja se on mahdollista selvittää esimerkiksi haittaohjelmilla (5). PIN-koodi on syötettävissä näppäimistöllisellä kulunvalvontalukijalla kuten kuvassa 2.



KUVA 2. Idescon näppäimistöllinen kulunvalvontalukija (6)

### 2.2.2 Etätunnistin

Etätunnistimen toiminta perustuu radiotaajuiseen etätunnistukseen eli RFID-tekniikkaan. RFID-tekniikassa tieto tallennetaan RFID-tunnistimeen, joka luetaan RFID-lukijalla radioaaltojen avulla. RFID-tunnistimia käytetään henkilöiden ja esineiden tunnistamiseen, havainnointiin ja yksilöintiin. (7.)

RFID-tekniikan etuna toimii kohteiden luettavuus kaukaa, nopeasti ja tietoturvallisesti. Lisäksi tunnisteet ovat uudelleenkirjoitettavia ja voivat sisältää paljonkin tietoa. Koteloidut tunnisteet

kestävät myös kovaakin käsittelyä ja voivat olla käyttökelpoisia jopa kymmeniä vuosia. Kulunvalvonnassa käytettävät etätunnisteet näyttävät yleensä kuvan 3 kaltaisilta. (7.)



*KUVA 3. Matalan taajuuden RFID-tunnisteita (8)*

### **2.2.3 Biometriset tunnisteet**

Biometrisissä tunnistusmenetelmissä käytetään hyväksi ihmisten kehosta löytyviä yksilöllisiä piirteitä. Esimerkiksi, arjen tietokoneissa ja älypuhelimissa on alettu käyttämään yleisesti biometrisiä tunnisteita, kuten sormenjälkeä, kasvoja ja silmiä (9). Vain hyvin harvoilla ihmisillä löytyy identtisiä biometrisiä tunnisteita, minkä takia henkilöiden tunnistaminen niiden avulla on hyvin varmaa. (10.)

Biometrisen tunnistamisen etuna on se, että ihminen kantaa biometrisiä tunnisteita aina mukanaan eikä niitä voida varastaa yhtä helposti kuin fyysisiä tunnisteita. Biometrinen tunniste on väärentäminen tuo kuitenkin ongelman. Jos henkilön biometrinen tunniste onnistutaan väärentämään, sitä ei voida ikinä enää käyttää luotettavana tunnisteena. Biometrinen tunnisteiden käyttäminen lisää myös mahdollisuuksia vakoilla yksittäisiä henkilöitä esimerkiksi valvontakameroiden avulla. Tämä voi heikentää ihmisten yksityisyyttä, mutta voi myös esimerkiksi estää mahdollista terrorismia. (11.)

Biometrinen tunnistaminen ei ole uusi juttu, mutta sitä on otettu enemmän käyttöön järjestelmien halventumisen ja luotettavuuden kehittymisen myötä. (12.) Biometrinen tunnistaminen nähdään kovaa vauhtia erityisesti maksutapahtumissa (9). Biometrinen tunnistautuminen nähdään maksamisessa turvallisempaa ja helpompaa (13). Vielä ei kuitenkaan ole täysin tietoa, mitä riskejä biometriset tunnistimet tuovat suuressa määrin käytettynä. Pelkkää biometristä tunnistetta käyttävä järjestelmä nähdään kuitenkin hyvin haavoittuvana. Siksi biometrisiä tunnistimia olisi hyvä lisätä vain PIN-koodin tai muun salasanan rinnalle. Biometrisessä tunnistautumisessa suurimpana riskinä on kuitenkin tunnistimien keräämiseen käytetyn rekisterin väärinkäyttö. (9.)

Erilaisia biometrisiä tunnistusmenetelmiä on useita. Yleisesti tiedossa olevia fysiologisia biometrisiä tunnistimia ovat esimerkiksi sormenjälki, kasvot, silmä, käsi, korva ja DNA. Käyttämiseen perustuvia biometrisiä tunnistimia ovat esimerkiksi allekirjoitus, puhe, kävelytyyli ja sydämen syke. Tässä osiossa käydään kuitenkin vain yleisimmät biometriset tunnistimet, jotka ovat yleisesti käytössä monissa paikoissa, sekä niiden hyötyjä ja haittoja. (14.)

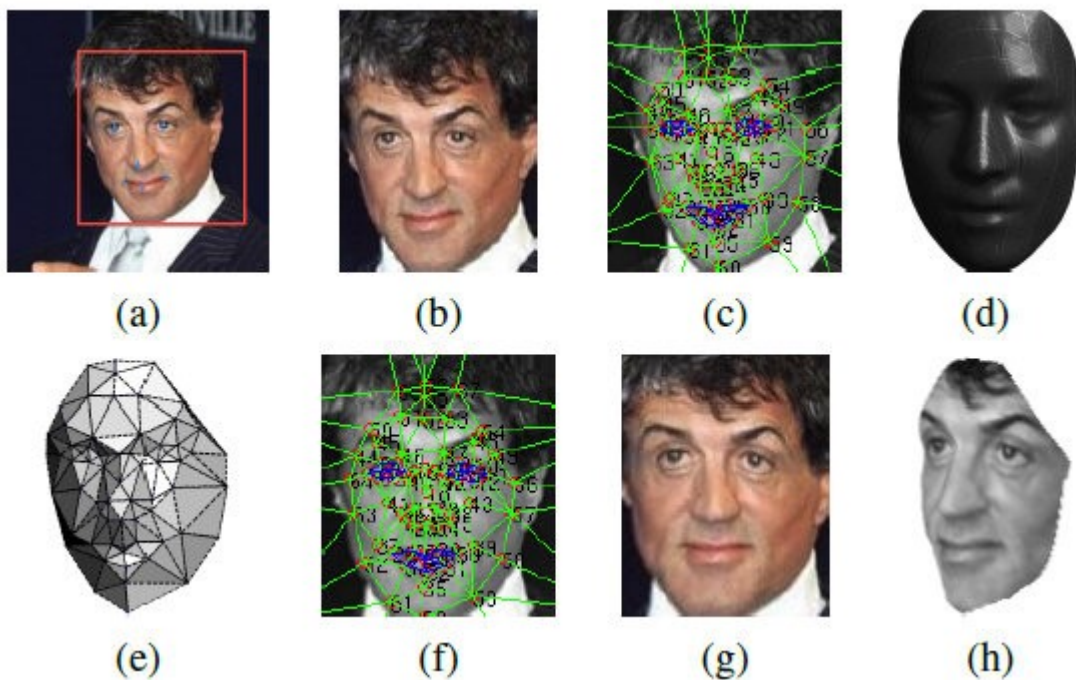
### **2.2.3.1 Sormenjälki**

Sormenjälkitunnistus on vanhin ja laajimmin levinnyt biometrinen tunnistusmenetelmä. Siksi sitä on ehditty kehittää hyvin pitkälle. (14.) Esimerkiksi nykyajan mobiilipankkeihin pääsee kirjautumaan sisälle jo pelkällä sormenjäljellä. Nykyajan älypuhelimien näyttöjen alta löytyy kameroihin tai ultraääneen perustuvia sormenjälkilukijoita. (15.) Myös joissain kuntosaleissa ja työpaikoissa ovi aukeaa sormenjäljellä (9).

Yksi sormenjälkitunnistuksen heikkouksista on sen kielteinen mielikuva sen yhdistämisestä rikollisten tunnistamiseen. Toinen heikkouksista on myös tunnistimen hämääminen ja sormenjäljen väärentäminen. Esimerkiksi sormenjäljen kopiaaminen juomalasista on täysin mahdollista. Sormenjäljen väärentäminen on kuitenkin vaikeaa ja sormenjälkitunnistimia kehitetään jatkuvasti estämään mahdollinen huijaaminen. (14.) Muualla kuin sisätiloissa ympäristötekijät voivat myös heikentää sormen luettavuutta, kuten kylmä tai kostea ilma.

### 2.2.3.2 Kasvot

Kasvojen tunnistus perustuu nykyaikana enimmäkseen kolmiulotteiseen kasvojen mittaamiseen. Kolmiulotteista kasvojen tunnistusta on vaikea huijata, sillä tunnistaminen perustuu ihmisen kasvonpiirteiden kovien kohtien välisien suhteiden mittaamiseen. Esimerkiksi plastiikkakirurgialla on hyvin vaikea muuttaa silmien välistä etäisyyttä toisistaan. (12.) Kasvojen tunnistuksessa kolmiulotteisella kasvokuvalla ihminen voidaan tunnistaa tehokkaammin kuin kaksiulotteisesta kuvasta, sillä sitä voidaan tarkastella useasta eri suunnasta ja kolmiulotteisesta kuvasta voidaan tunnistaa enemmän ihmisiä yksilöiviä piirteitä (11). Esimerkiksi kuvassa 4 Facebookin tekoälyä käyttävä DeepFace-teknologia luo kaksiulotteisesta kuvasta kolmiulotteisen mallin, jota teknologia käyttää tunnistamiseen (16). Kolmiulotteinen kasvojentunnistus on ainoa biometrinen tunnistusmenetelmä, joka voidaan tehdä passiivisesti kohteen huomaamatta (11). Kasvojentunnistuksessa yksi heikkouksista on kuitenkin se, että ihmisen pään muoto voi muuttua ihmisen vanhetessa. (12.)



KUVA 4. Facebookin DeepFace-teknologian toimintatyylä (16)

Kasvojen tunnistusta voidaan käyttää laajojen ihmismassojen skannaamiseen massatapahtumissa, kuten konserteissa tai urheilutapahtumissa. Terrorismiuhkat ovat lisääntyneet nykyaikoina ja siksi kasvojen tunnistusta halutaan käyttää myös terrorismin torjunnan yhtenä

menetelmänä. Yleisesti kasvojen tunnistusta käytetään kuitenkin älypuhelisten ja tietokoneiden lukituksen avaamiseen ja se halutaan ottaa laajemmin käyttöön lentokentillä, juna-asemilla ja maiden rajoilla nopeuttamaan ja tehostamaan valvontaa. (17.)

#### **2.2.3.3 Silmä**

Silmän iiriksen tunnistamista pidetään luotettavana biometrisenä tunnistustapana, sillä se on erittäin tarkka. Silmien iiriksiä skannaavia tunnistimia on käytetty jo monia vuosia passintarkastuksessa, mutta iiriksen tunnistavia infrapunakameroita on lisätty älypuheliin vasta viime vuosina. (9.) Iristunnistus toimii kameraa katsomalla ja kestää muutaman sekunnin, jos puhelimeen on tallennettu kuva käyttäjän silmistä. Iristunnistus on hyvä biometrinen tunnistus, jos halutaan kiinnittää tietoturvaan enemmän huomiota. (18.) Iristunnistuksen heikkouksena on kuitenkin se, että silmän iiriksestä otettua tunnistekuvaa joutuu päivittämään säännöllisesti, sillä se muuttuu iän myötä (19).

#### **2.2.4 Mobiilitunnistin**

Älypuhelimista on tullut osa meidän jokapäiväistä arkea (1). Tilastokeskuksen mukaan vuonna 2020 alle 55-vuotiaista jopa yli 98 prosenttia käytti älypuhelimia (20). Älypuhelisten käyttäjämäärät ovat jatkaneet kasvamistaan vuosi vuodelta (21).

Nykyaikana arkipäiväisten toimintojen keskittäminen älypuheliin tuntuu luontevalta, koska älypuhelimia pidetään jatkuvasti mukana. Esimerkiksi älypuhelimien käyttö maksuvälineenä on yleistynyt. Maksusovelluksen käyttö ei vaadi isoja toimenpiteitä ja sen asentaminen on nopeaa. Tunnistin asennetaan jo ennestään tuttuun laitteeseen, joten uusien laitteiden tai tunnistimien käyttöä tai opettelua ei tarvita (22). Mobiilitunnistimien heikkous on kuitenkin puhelimien akkujen rajallisen virran määrä. Puhelimen akun loppumisen kannalta on hyvä pitää varalta mukana myös tavallisia tunnistimia.

Tunnistin digitaalisessa muodossa on hyvin joustava ratkaisu, sillä tunnistin on mahdollista vaihtaa ja päivittää helposti ja edullisesti. Älypuhelimien Bluetooth- ja NFC-teknologiat mahdollistavat myös tunnistamisen eri etäisyyksiltä. Älypuhelimien tehokkuuden avulla on myös mahdollista piilottaa tunnistukset salausalgoritmeilla, joiden purkaminen on aikaa vievää ja vaikeaa.



## **2.2.5 Mahdolliset tulevaisuuden tunnistimet**

Erilaisten uusien arjen laitteiden suosio kasvaa ajan myötä ja niiden käyttäminen tunnisteena on mahdollista. Laitteiden kokovaatimusten pienentyessä ollaan kehitetty uusia yleensäkin kehoon kiinnitettäviä laitteita, kuten älykelloja, älysormuksia, erilaisia älyvaatteita ja ihon alle kiinnitettäviä siruja. Myös aivoihin kiinnitettävät tekoälylaitteet ovat kehitteillä.

Älyvaate on jokin puettava vaatekappale tai asuste, johon on lisätty elektroniikkaa. Älyvaatteissa voi olla esimerkiksi antureita, jotka tunnistavat henkilön ja samalla ilman lämpötilan. Näiden tietojen avulla vaatteet voivat esimerkiksi säätää omaa lämpötilaa tarpeen mukaan. Näistä antureista saatavat tiedot joissain paikoissa voidaan myös lähettää työpaikan järjestelmiin. Samoja vaatteita olisi mahdollista käyttää esimerkiksi kulunvalvonnassa kyseisen henkilön tunnistamiseen rakennuksen sisään tullessa. (23.)

Esimerkiksi älykelloissa ja älysormuksissa on jo olemassa Bluetooth- ja NFC-kommunikaatiomahdollisuus, joten niiden käyttö yleisenä tunnistimena on mahdollista. Jos tunnistaminen vaatii laitteen omistajalta interaktiivisuutta laitteen kanssa, on älysormuksen tai älykellon käyttö sujuvampaa kuin esimerkiksi älypuhelimien kaivaminen taskusta. Älykellolle puhumista olisi myös mahdollista käyttää tunnistusmenetelmänä. Älykellojen käyttö on kuitenkin pysynyt melko pienenä, vaikka erilaisten älykellojen ja -rannekkeiden määrä on lisääntynyt (21). Muun muassa älypuhelimien jo ennestään laajat toiminnallisuudet ja älykellojen pieni näyttö syövät älykellojen suosiota (24).

## **2.3 Pohdinta tunnistusmenetelmistä**

Pidämme älypuhelimia jatkuvasti mukanaamme. Siksi niiden käyttäminen arkipäiväisiin toimiimme tuntuu luontevalta. Älypuhelimien käyttämät radiotaajuuudet mahdollistavat vakaan yhteyden pitkältikin etäisyydeltä ja yhteystekniikat ovat kevyitä. Nykyajan puhelimien tehokkuuden avulla on myös mahdollista piilottaa kommunikoinnit salausalgoritmeilla, joiden purkaminen on aikaa vievää ja vaikeaa.

Helpot sovellusten asennus- ja päivitysmahdollisuudet antavat hyvät laajennusmahdollisuudet mobiilitunnisteelle. Mobiilitunnisteen digitaalista sisältöä on helppo muuttaa ihan toimintatavoista

käyttäjän tunnistimeen. Jatkuva edestakainen kommunikointi lukijoiden kanssa mahdollistaa myös muidenkin tietojen, kuten lukijoihin asetettujen sääntöjen tai arvojen, jakamisen. Mobiilitunnistimen ratkaisusta voi siis tehdä hyvinkin joustavan käyttäjän tilanteisiin nähden.

Älypuhelimien käyttö tunnisteena ei vaadi käyttäjältä muistitietoa eikä välttämättä edes kosketusta. Älypuhelimeen on kuitenkin mahdollista lisätä puhelimen omia suojauskeinoja, kuten sormenjälki, kasvojen tunnistus tai PIN-koodi. Älypuhelimien heikkous on kuitenkin sen akun kesto. Puhelimen virran loppumisen kannalta kannattaa pitää varalta mukana esimerkiksi myös etätunnistinta. Mobiilitunnistin ei estä aikaisempien tunnistimien käyttöä kulunvalvontajärjestelmässä. Mobiilitunnistin toimii säällä kuin säällä eikä vaadi fyysistä kosketusta laitteisiin, joten se on myös hyvin hygieeninen. Digitaalisena tunnistimena se ei myöskään vanhene kuten osa biometrisistä tunnistimista. Älypuhelimien suosio kasvaa entisestään eikä älypuhelinta korvaavaa laitetta näyttäisi tulevan lähitulevaisuudessa. Mobiilitunniste on hyvä välimuoto turvallisuuden ja käytettävyyden välillä.

### 3 PUHELIMESTA LÖYTYVÄT TUNNISTEET

Projektin alussa oli tarkoitus tehdä esitutkimusta mahdollisimman yksilöllisen tunnisteen luomisesta puhelimen tiedoista niin, että jokaisen käyttäjän puhelin pysyisi tunnisteeltaan henkilökohtaisena eikä esimerkiksi muuttuisi uudelleenasetuksen tai tehdasasetuksien palautuksen myötä. Samalla tutkittiin sitä, kuinka näitä puhelimen yksilöllisiä tietoja voitaisiin käyttää keskenään ilman tunnistimen pituuden kasvamista liian pitkäksi. Myös eri puhelinversioiden tuoma vaikutus tietojen saantiin oli tutkittava.

#### 3.1 Secure Android ID

Laitteen ensimmäisellä käynnistyksellä laitteessa luodaan 64-bittinen satunnainen arvo, joka pysyy samana laitteen elinkaaren ajan. Tämä tunnetaan nimellä Android ID, joka on vaihtoehto yksilöllisen laitteen tunnistamiseksi. Android ID:n käytössä on kuitenkin ongelma. Android ID saattaa muuttua tehdasasetusten palautuksessa ja tiedossa on myös virhe, jossa tietyllä määrällä saman puhelinvalmistajan puhelimista on sama Android ID. (25.) Android ID myös mahdollista muuttaa puhelimesta, johon on sallittu root- eli pääkäyttäjäoikeudet (26). Root-käyttäjä tunnus on Unix-järjestelmässä pääkäyttäjä, jolla on oikeus muuttaa kaikkea laitteesta saatavilla olevaa tietoa. Älypuhelimissa root-oikeuksien salliminen eli "roottaus" aiheuttaa puhelimen takuuoikeuksien menettämisen, sillä roottaus voi aiheuttaa laitteen järjestelmän menemisen "solmuun" ja sen palauttaminen alkuperäiseen tilaansa vaatii käyttöjärjestelmän uudelleenasetamisen. Varmuuskopion tekeminen ennen roottausta on suositeltavaa. (27.)

Androidin versiosta 8.0 eteenpäin Android ID muuttuu yksilölliseksi jokaiselle sovellukselle ja käyttäjälle laitteen sisällä. Tämä sovelluskohtainen Android ID ei kuitenkaan muutu sovelluksen uudelleenasetuksen yhteydessä niin kauan kuin paketin nimi ja allekirjoitusavain pysyvät samana. Sovelluksen Android ID pysyy myös samana, jos vanhempi Android päivitetään versioon 8.0 tai uudempaan. Androidin päivittämisen jälkeen Android ID muuttuu sovelluksen uudelleenasetamisen yhteydessä. (28.)

### 3.2 UUID

UUID eli Universally Unique Identifier on 128-bittinen generoitava arvo, jolla voidaan tunnistaa tietty sovelluksen asennus. UUID ei kuitenkaan määritä itse laitetta ja arvo täytyy tallentaa, jotta käyttäjä voidaan tunnistaa seuraavalla kerralla sovelluksen käynnistyessä. (25.)

### 3.3 IMEI, MEID, ESN, IMSI

IMEI on 15-numeroinen yksilöllinen tunnus, joka on mahdollista saada puhelimesta, jossa on puhelujensoitto-ominaisuus. IMEI on SIM-kortin paikasta riippuvainen tunnus, joka pysyy samana, vaikka laitteen sovellus uudelleenasetettaisiin. IMEI pysyy myös samana, jos laite palautetaan tehdasasetuksiin tai laite rootataan. Laitteesta, johon on sallittu root- eli pääkäyttäjäoikeudet, on mahdollista muuttaa IMEI-arvoa, mutta joissain maissa IMEI:n vaihtaminen on lailla kiellettyä. IMEI:n muuttamisen jälkeen laitteen seuranta ja sen korvaaminen ei ole enää mahdollista. Laitteessa on myös mahdollista olla useampi IMEI, jos laitteessa on monta SIM-korttipaikkaa. Jotta voidaan selvittää ohjelmakoodin kautta IMEI laitteesta, on käyttäjän sallittava sovellukselle oikeus lukea puhelimen tilaa. (25.)

### 3.4 MAC- ja Bluetooth-osoite

Laitteilta, joista löytyy Wi-Fi - tai Bluetooth-laitteisto, on mahdollista saada laitteen 48-bittinen Internet-kommunikoinnissa käytettävä yksilöllinen MAC-osoite, joka tulee sanasta Media Access Control. Androidilla on kuitenkin tarkoitus estää mahdollista MAC-osoitteen hankkimista ohjelmakoodin kautta. (25.) Sinänsä tämä ei muutenkaan ole hyvä vaihtoehto salaisena tunnuksena, sillä Bluetooth-laitteiston ollessa päällä laite mainostaa omaa MAC-osoitetta yleisesti kaikille toisille laitteille. MAC-osoitteen voi myös muuttaa samaksi laitteesta, johon on sallittu root- eli pääkäyttäjäoikeudet (29). Nykyään on muutenkin parempia tunnusvaihtoehtoja saatavilla (25).

### 3.5 Sarjanumero

Sarjanumero on valmistajan luoma yksilöllinen tunnus laitteen seurantaan, enimmäkseen korjaus- ja takuuasioihin liittyen. Sarjanumeron voi yleensä löytää tuotelaatikon kyljestä eli se ei ole kovinkaan salainen tunnus, mutta sen jakaminen muille voi aiheuttaa ongelmia, kuten tuotetakuun

menettämisen. (30.) Sarjanumero on myös muutettavissa laitteesta, johon on sallittu root- eli pääkäyttäjäoikeudet (31).

### **3.6 Advertising ID**

Advertising ID on yksilöllinen tunnistin, jota suositellaan käytettävän vain käyttäjä- tai mainosseurantaan liittyvissä tarpeissa. Tätä tunnistinta käytettäessä sitä ei saa yhdistää henkilön tai laitteen henkilökohtaisiin tunnistettaviin tietoihin ilman käyttäjän suostumusta. Jos Advertising ID resetoidaan, ei se saa olla myöskään missään yhteyksissä aikaisempaan tunnisteeseen tai aikaisemmalla tunnisteella tehtyihin muutoksiin ilman suostumusta. Advertising ID:n käyttökohteiden täytyy olla myös käyttäjän tiedossa. (32.)

### **3.7 Instance ID**

Instance ID on yksilöllinen tunnistin yksittäisen sovelluksen tunnistamiseen. Instance ID pysyy samana, jos itse sovellus ei poista Instance ID:tä, laitetta ei vaihdeta, sovellusta ei uudelleenasetenneta tai sovelluksen tietoja ei poisteta. (33.)

### **3.8 Tunnisteiden pohdinta**

Tietoturvallisuuden vuoksi tässä osiossa ei ole tarkoitus käsitellä opinnäytetyössä käytettyä ratkaisua tunnuksien käytöstä vaan kertoa tunnuksien hyvistä ja huonoista puolista yleisesti. Tunnisteiden tutkinta projektia varten jatkui laajemmin myös tämän opinnäytetyön ulkopuolella.

Kulunvalvonnassa, jos käyttäjä menettää henkilökohtaisen tunnistimensa, on hänen käytävä rekisteröimässä uusi tunnistin järjestelmään järjestelmävastaavalla. Siksi tunnisteiden käyttämisessä olisi tärkeää, että käyttäjälle luotu tunnistin säilyisi samana myös sovelluksen uudelleenasetamisessa. Tämä ongelma tulee esille varsinkin isoissa käyttäjäkunnissa, joissa käyttäjiä voi olla satoja tai jopa tuhansia. Mitä isompi määrä käyttäjiä, sen todennäköisempää, että uudelleenasetamisia ja rekisteröintikäyntejä tulee järjestelmävastaavalle.

Tunnisteiden käytön turvallisuutta lisää myös mahdollisimman monen puhelimesta löytyvän tunnisteiden käyttö. Jos käyttäjätunniste on luotu esimerkiksi yhdestä puhelimesta löytyvästä

tunnistelähteestä, on tunnistinlähde helpommin tunnistettavissa ja vaihdettavissa samaksi puhelimessa, johon on sallittu root- eli pääkäyttäjäoikeudet. Useamman tunnistelähteen käyttäminen lisää kuitenkin käytettävän käyttäjätunnisteen pituutta. Kun käyttäjätunniste on liian pitkä, on sitä lyhennettävä, mikä taas lisää mahdollisuutta duplikaatteihin. Käyttäjän tunnistamiseen käytettävän tunnisteen pituus riippuu täysin kulunvalvontajärjestelmästä ja se vaihtelee paljonkin eri järjestelmissä, mutta yleisimmät tunnistimen pituudet ovat 32 bittiä ja 56 bittiä.

Kehitysvaiheessa oltiin myös huolissaan tulevan Android 10 -käyttöjärjestelmän tuomasta ongelmasta. Android 10 toi rajoituksia puhelimesta löytyviin laitetunnisteisiin, joita ei ole mahdollista resetoita. Näihin tunnisteisiin kuuluvat muun muassa IMEI ja sarjanumero. Android siten suosittelee tunnistimiksi joko mainosseurantaan käytettävää Advertising ID:tä tai yksittäisen sovelluksen tunnistamiseen käytettävää Instance ID:tä. (34.)

## 4 MOBIILIRATKAISUT MARKKINOILLA

Projektin alussa oli tarkoitus tehdä esitutkimusta markkinoilla olevista mobiiliratkaisuista. Sen avulla oli helpompi suunnitella, miten älypuhelimien käyttöönotto kulunvalvontaan tullaan ratkaisemaan. Asiakkaiden antamat käyttäjäkokemukset toisten yritysten markkinoilla olevista tuotteista otettiin myös suunnitelmissa huomioon.

### 4.1 HID

HID on vuonna 1991 perustettu amerikkalainen turvallisuuteen perustuvia identifiointituotteita valmistava yhtiö ja ruotsalaisen lukkovalmistajan Assa Abloyn tytäryhtiö (35). HID valmistaa mobiiliratkaisuna HID Mobile Access -tuotetta (kuva 5), jolla asiakkaat voivat käyttää älypuhelimia, tablettia tai puettavaa esinettä yleiseen kulunvalvontaan (36).

HID Mobile Access -tuotteen avulla asiakkaat voivat päästä erillisen kortin sijasta mobiililaitteellansa etenemään lukituista ovista. HID:n tuotteen yhteen toimintatapaan kuuluu sovelluksen ”Tap”-liike, jossa HID:n lukijasovellus avataan ja puhelinta ”täpätään” lukijaan eli puhelin viedään lukijan lähelle. Toinen toimintatapa on HID:n patentoima ”Twist and Go”-liike, jossa etäällä puhelin käännetään kylkiasentoon oven aukaisua varten. HID:n sovelluksen käyttö vaatii pilvipalvelun eli myös verkkoyhteyden käytön ja titlitetojen hankkiminen hoituu kuukausimaksuilla. HID Mobile Access on korkeamman tason pilviratkaisu puhelimen käyttöönottoon kulunvalvonnassa. (36.)



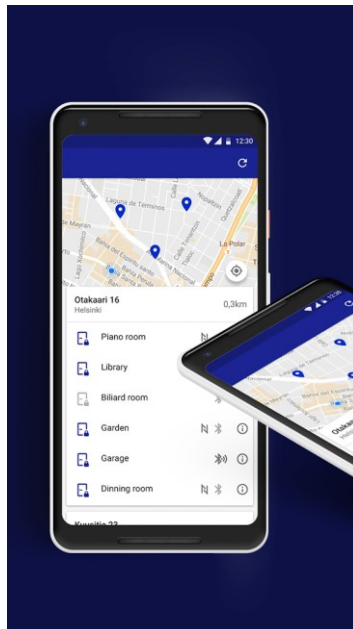
KUVA 5. HID Mobile Access -sovellus ja HID:n kulunvalvontalukija (36)

## 4.2 Bitwards

Bitwards Oy on vuonna 2016 perustettu suomalainen startup-yritys, jonka päätoimipaikka sijaitsee Helsingissä. Bitwards kehittää yrityksille, yhteisöille sekä yksittäisille ihmisille digitaalisia palveluita sekä teknologioita. (37.)

Bitwardsilla on palvelu nimeltään Access Sharing Service (kuva 6), joka parantaa erilaisten laitteiden ja palveluiden yhteiskäyttöä. Palvelulla voidaan ratkaista useampi pääsynhallintaratkaisuihin esiintyvä ongelma, esimerkiksi fyysisten avainten käyttö sekä niiden hallinta. Palvelun käyttökohteita ovat liikkumisen palvelut, kuten polkupyörien ja autojen yhteiskäyttöpalvelut sekä kokoustilojen, vuokrattavien tilojen ja majoituspalveluiden yhteiskäyttö. Myös erilaisten ovien, kaappien, älykkäiden laitteiden sekä automaattien käyttöoikeuksien hallinta on mahdollista. (37.)

Bitwards Access Sharing Servicessä pääsy kulunvalvontaan ostetaan pääsykorttien sijasta digitaalisena tilitietona Bitwardsin pilvipalvelusta. Sovellus vaatii siten myös verkkoyhteyden ja pilvipalveluun rekisteröitymisen toimiakseen. (38.) Sovellukseen rekisteröidään asiakkaan omistamat lukijat ja niiden avaus käy etäältä sovelluksen lukijalistasta tai NFC-yhteydellä tuomalla älypuhelin lukijan lähelle.



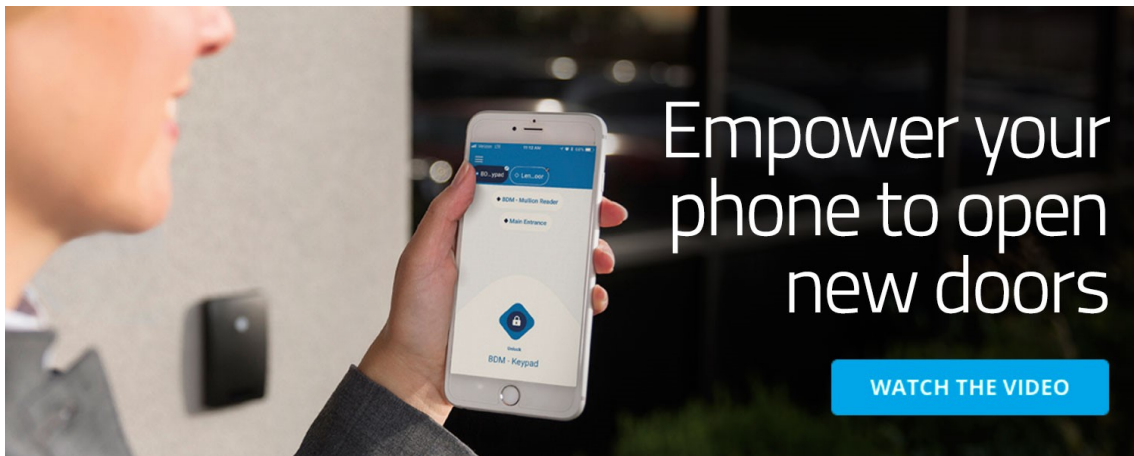
KUVA 6. Bitwards Access Sharing Service -sovelluksen päänäköymä (39)



### 4.3 Lenel

Lenel on vuonna 1991 perustettu maailmanlaajuinen turvallisuusjärjestelmiin keskittyvä yritys (40). Lenelin lukituslaitteita on laajalti asennettu useille teollisuudenaloille 17 vuoden ajan (41).

Lenelin kehittämä BlueDiamond Mobile -ratkaisu (kuva 7) yhdistää älypuhelimien käytön saumattomasti kulunvalvontaan Bluetooth Low Energy -tekniikalla. BlueDiamond Mobile tarjoaa sovelluksen, BlueDiamond Mobile Bluetooth- ja RFID-lukijat sekä BlueDiamond Mobile -tilitiedot yhdistettynä toisiinsa pilvipalvelun kautta. (41.) BlueDiamond Mobile -ratkaisu tuo myös uuden Pathways-ominaisuuden, joka sallii GPS-tekniikan avulla helpon pääsyn aikaisemmin määritettyyn polkuun rakennuksessa, esimerkiksi kokoushuoneeseen tai omaan toimistoon (42).



KUVA 7. Lenel BlueDiamond Mobile -sovellus (41)

### 4.4 STid

STid on turvallisuustekniikoihin keskittyvä maailmanlaajuinen yritys, joka tuottaa turvallisuusratkaisuja yrityksille. STid perustettiin vuonna 1996 ja sen pääkonttori sijaitsee Ranskassa. (43.)

STid tuo mobiiliratkaisunaan STid Mobile ID -tuotteensa (kuva 8). Ratkaisullaan STid antaa uusia erilaisia käyttötapoja mobiilitunnistamiseen kulunvalvonnassa. Näitä käyttötapoja ovat muun muassa "Card", "Remote", "Slide", "Hands-free" ja "Tap Tap" -moodit. "Card"-moodissa puhelinta käytetään kulunvalvontakorttina eli puhelinta näytetään lukijalle. "Remote"-moodissa STidin mobiilisovelluksesta painetaan nappia oven avaamista varten. "Slide"-moodissa kättä liu'utetaan

lukijan päällä oven avaamiseksi eikä itse puhelinta tarvitse ottaa esille. "Hands-free"-moodissa taas riittää, että kävellään lukijan ohi avatakseen lähellä olevan oven. "Tap Tap"-moodissa voidaan avata lähimmän oven taputtamalla taskussa olevaa puhelinta kahdesti. Lukijat voidaan myös asettaa käyttämään eri moodeja etäisyyksien mukaan. (44.)

STid Mobile ID vaatii virtuaalisen kortin asentamisen toimiakseen. Virtuaalikortti asennetaan sovellukseen joko ilman verkkoyhteyttä paikallisesti tai verkkoyhteyden välityksellä. Virtuaalikorteista ilmainen versio sisältää vain "Card"-moodin eli puhelimen lukijalle näyttämisen ja maksulliset virtuaalikorttiversiot sallivat useamman moodin käyttämisen lukijoissa. Järjestelmässä käytettävä henkilökohtainen ID ei sijaitse itse sovelluksessa. (44.)



KUVA 8. STid Mobile ID -sovellus ja STidin kulunvalvontalukija (44)

#### 4.5 Nedap

Nedap on Alankomaissa perustettu yritys, joka toimii monella eri teknologian alalla (45). Nedap on perustettu vuonna 1929 ja toimii maailmanlaajuisesti 127 maassa (46).

Nedapin mobiiliratkaisu on nimeltään MACE eli Mobile Access Control Entities (kuva 9). Se on alusta, joka sallii minkä tahansa älypuhelimien käyttämisen tunnistena pääsykontrollijärjestelmässä. Alusta sisältää pilvipalvelun, lukijat sekä sovellukset. Sovellukset

voivat sisältää useammat virtuaaliset tilitiedot ja ne voidaan siirtää sovelluksesta lukijalle joko NFC:llä, BLE:llä tai QR-koodilla. (47.)

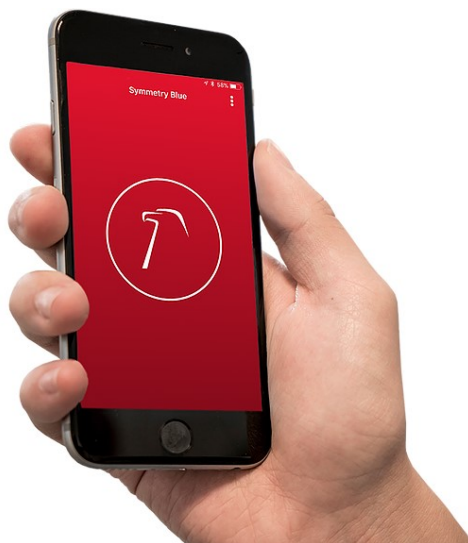


KUVA 9. Nedap MACE -sovellus ja Nedapin kulunvalvontalukija (48)

#### 4.6 AMAG

AMAG Technology on turvallisuusalan yritys, joka tarjoaa turvallisuuspalveluita kulunvalvontaan. AMAG kuuluu G4S-konserniin ja toimii aktiivisesti yli sadassa maassa. (49.)

AMAG:n älypuhelinratkaisu kulunvalvontaan on nimeltään Symmetry Blue (kuva 10). Symmetry Bluen sovellus itsessään ei maksa mitään eikä vaadi lisenssiä toimiakseen. Symmetry Blue -lukija voi lukea BLE-tilitiedot läheltä sekä myös kaukaa. (50.)



KUVA 10. Symmetry Blue -ratkaisun mobiilisovellus (51)

#### 4.7 Mobiiliratkaisujen pohdinta

Suunnitellussa Idesco Mobile Lite -ratkaisussa pyritään mahdollisimman helppokäyttöiseen ja käyttäjäystävälliseen mobiiliratkaisuun kulunvalvonnassa. Tiedossa olevat markkinoiden älypuhelinratkaisut eivät anna haluttua täysin käyttäjäystävällistä kokemusta. Esimerkiksi sovelluksien käyttö on hidasta, vaativat Internet-yhteyttä toimiakseen tai vaativat liian monta välivaihetta oven aukaisuun. Tällä projektilla pyritään ratkaisemaan tämä ongelma.

Kaikissa tiedossa olevista markkinoiden älypuhelinratkaisuista itse mobiilisovellusta käytetään ovien aukaisemiseen. Tämä tuo lisävaiheita, kuten sovelluksen etsimisen sovelluslistasta ja sovelluksen aukeamisen odottamisen. Joissakin markkinoiden ratkaisuissa vielä itse sovelluksessa joudutaan selaamaan ovilistoja, jotka saattavat sisältää myös ovia, jotka eivät ole edes lähialueella. Idesco Mobile Lite on kuitenkin suunniteltu toimimaan taustalla ja ovien hallinta integroituna sulavasti itse käyttöjärjestelmään. Jotkut ratkaisut käyttävät myös sovelluksen sijaan erilaisia sovelluksen ulkopuolisia käyttötapoja, kuten puhelimen gyroskooppia mikä on nähty käytännössä vain epävarmuutta tuovalta kosmeettiselta ratkaisulta.

Idesco Mobile Liten tarkoitus on siis olla kevyemmän turvallisuustason ratkaisu eli se ei tarvitse kolmatta osapuolta, esimerkiksi pilveä tai ulkoista tietokantaa, toimiakseen. Mobile Lite -sovellus on myös täysin ilmainen eikä vaadi käyttäjältä pilveen rekisteröitymistä eikä lisenssejä toimiakseen. Pilvipalveluiden käyttö tai niihin rekisteröityminen vaatii aina verkkoyhteyden. Monet yritykset eivät halua kolmannen osapuolen hallintaa turvallisuusratkaisuihinsa. Mobile Lite nähdään yleisesti etätunnistimen korvikkeena.

Idesco Mobile Litessä on ainutlaatuista vielä sen joustavuus konfiguroitavilla asetusarvoilla. Asetusarvoilla on mahdollista säätää lukijan lähellä olevien mobiilitunnisteiden käyttäytymistä.

## 5 TOTEUTUS

### 5.1 Lähtötilanne

Olin aikaisemmin toteuttanut Idescolle yrityslähtöisen tuotekehitysprojektin ja minulle alettiin tutkimaan uutta projektia työn alle. Idesco oli kiinnostunut ja selvittänyt, miten matkapuhelinta olisi mahdollista käyttää monimuotoisena tunnisteena, osana kulunvalvontajärjestelmää, RFID-tunnistimen rinnalla.

Annetun työn lähtötilanteena oli suunnitella ja toteuttaa mahdollisimman helppokäyttöinen BLE-mobiilialusta ratkaisuna mobiililaitteen käyttöönottoon kulunvalvonnassa. Alustasta toivottiin mahdollisimman kevyt ja sen haluttiin toimivan myös ilman ulkoista pilveä tai tietokantaa. Sovellus ei vaatisi Internet-yhteyttä eikä kirjautumista toimiakseen. Sovelluksesta haluttiin matalamman turvatason kulunvalvontaratkaisu Idescon korkeamman tason pilvisovelluksen rinnalle.

Tarkoituksena oli käyttää lukijan kanssa kommunikointiin BLE- eli Bluetooth Low Energy -tekniikkaa. Sovelluksen avulla oli tarkoitus käyttää puhelimesta löytyviä sisäisiä tunnisteita ja tietoja luomaan kulunvalvontaan yksilöllinen puhelinkohtainen tunniste, joka ei myöskään vaihdu uudelleenasetuksen yhteydessä. Sovellus olisi vapaasti ladattavissa sovelluskaupasta ja oikeudet kulunvalvontaan annettaisiin vain järjestelmänhallitsijan kautta. Projektin toteutukseen alettiin käyttää Idescon sisäistä prosessimallia.

### 5.2 Vaatimusmäärittely

Idesco BLE Lite -alkuperäisessä hahmotelmassa oli tarkoitus toteuttaa Idescon lukijoille tuki NFC/BLE-kommunikaatiolle, jolla saadaan siirrettyä seitsemäntavuinen data mobiilisovelluksesta. Tarkoitus oli tehdä mobiilisovellus, joka on täysin vapaasti ja ilmaiseksi ladattavissa sovelluskaupasta. Sovelluksessa generoidaan yksilöllinen puhelinkohtainen ID puhelimen sisäisiä tietoja käyttäen. Demo ei ole minkäänlaisessa yhteydessä pilveen, ei vaadi rekisteröitymistä ja toimii täysin ilman Internet-yhteyttä. Lukijan käyttämät asetukset määritetään konfiguraatiokortilla tai järjestelmän kautta lukijalle. Idesco BLE Lite on helppokäyttöinen, mutta ei korkeinta turvatasoa oleva ratkaisu kulunvalvontaan. Vaihtoehtona voi käyttää Idescon pilvipohjaista ratkaisua

saadakseen korkeamman turvallisuuden. Graafisesti sovellus toteutettaisiin Idescon teemalla ja ohjeistuksella kuten kuvassa 11. Lisävaatimuksena sovellus tukisi myös mahdollisimman vanhoja Android-versioita. Käyttöliittymä olisi myös mahdollisimman yksinkertainen.



*KUVA 11. Idescon aikaisemmin suunnittelema graafinen demo Idescon brandilla ja tyyllillä*

### **5.3 Esiselvitys**

Esiselvityksenä selvitettiin, minkälaisia ratkaisuja Idescon kilpailijat olivat toteuttaneet markkinoille. Tutkimuksen kohteena olivat myös puhelimista löytyvät yksilölliset tunnisteet ja niiden saatavuus eri puhelinmalleista. Tutkimuksen kohteena olivat myös kulunvalvontajärjestelmät ja niiden käyttämät datamäärät mobiilitunnistetta varten, sillä vanhat järjestelmät tukevat suhteellisen pieniä datamääriä. Erilaisia kulunvalvontajärjestelmien käyttämiä tiedonsiirtoprotokollia on myös useita, joista yleisimpiä ovat Wiegand, RS-232, RS-485, Clock and Data ja Ethernet. Myös Idescon sisäinen kyselytutkimus sovelluksen tärkeistä ominaisuuksista ja vaatimuksista toteutettiin taustakartoituksena ja siihen osallistui 14 Idescon työntekijää. Akku ja viive oven avaamiseen näyttivät olevan tärkeimpiä ominaisuuksia kyselyn perusteella. NFC-ominaisuus oli myös haluttu ominaisuus ja älypuhelimeen luotetaan yleisesti tunnistimenä. Kyselyssä kysyttiin työntekijöiden liikkumisen seuraamista, mikä ei niinkään näyttänyt työntekijöitä häiritsevän, mutta erillisiä kommentteja tilanteista, missä sitä ei hyväksyttäisi, tuli kyllä. Työntekijöiden seuranta on kuitenkin itse järjestelmänhallitsijan vastuulla. Kyselytutkimuksen tulokset löytyvät opinnäytetyön liitteestä 1.

### **5.4 Ratkaisun suunnittelu**

Idescolla annettiin suunnitteluun hyvin vapaat kädet. Aloin suunnittelemaan älypuhelimien käyttöönottoa kulunvalvonnassa mahdollisimman helppokäyttöiseltä kannalta. Ratkaisusta oli

tulossa mahdollisimman kevyt, ovien aukaisemisesta mahdollisimman helppoa ja käytettävyys integroituna osaksi puhelimen käyttöjärjestelmää. Joustavuutta tulisi mobiilitunnisteen toimintasäännöillä, jotka ovat vaihdettavissa lukijakohtaisesti konfiguraatiokortilla.

Idesco Mobile Lite on luotu toimimaan taustalla. Sovelluksen käynnistämisen jälkeen käyttäjän ei tarvitse aukaista sovellusta, vaan käyttäjä voi avata ovet puhelimen ilmoituksien kautta. Itse ovien kontrollointiin on suunniteltu erilaiset toimintasäännöt. Lukijaan tallennettavia sovelluksen toimintaa ohjaavia parametreja on neljä kappaletta. "Security level" määrittää turvallisuustason, joita on suunniteltu kolme kappaletta. Yksi parametreista on "friendly name" eli lukijan nimi. "Threshold" säätää etäisyyden, jonka sisällä sovellus tunnistaa lukijan. "Re-read delay" on aika, jonka jälkeen ovi voidaan aukaista uudestaan samalla laitteella. Nämä sovellusta kontrolloivat tiedot on mahdollista lisätä lukijaan lukijan konfiguraatiokortilla. Nämä parametrit ovat pelisääntöjä, jotka määrittävät, miten mobiilisovellus käyttäytyy missäkin tilanteessa. Sovellus on ladattavissa ilmaiseksi puhelimen sovelluskaupasta ja sovelluksen luoma yksilöllinen tunniste voidaan siirtää kulunvalvontajärjestelmään opetuslukijalla. Opetuslukija on järjestelmänhallitsijan käytössä ja käyttäjän käyttöoikeuksia voidaan hallita kulunvalvontajärjestelmästä.

Suunniteltuun ratkaisuun turvatasoja tuli kolme. Turvatasoilla on mahdollista säätää haluttua turvallisuutta ja mukavuutta lukijakohtaisesti. Ensimmäinen turvataso on turvatasoista matalin eikä vaadi käyttäjältä toimenpiteitä, vaan oven aukaisemiseen riittää, että käyttäjä kävelee puhelimensa kanssa lukijaan tallennetun "threshold"-arvon määrittämälle alueelle. Puhelin voi olla taskussa, mikä helpottaa esimerkiksi sairaalatyöntekijöitä kiireisissä tilanteissa, joissa ylimääräisiä käsiä ei ole helposti saatavilla. Tämä turvallisuustaso on suositeltavana vain sisätiloihin, välioville tai oville, joiden turvatasolla ei ole suurempaa vaatimusta.

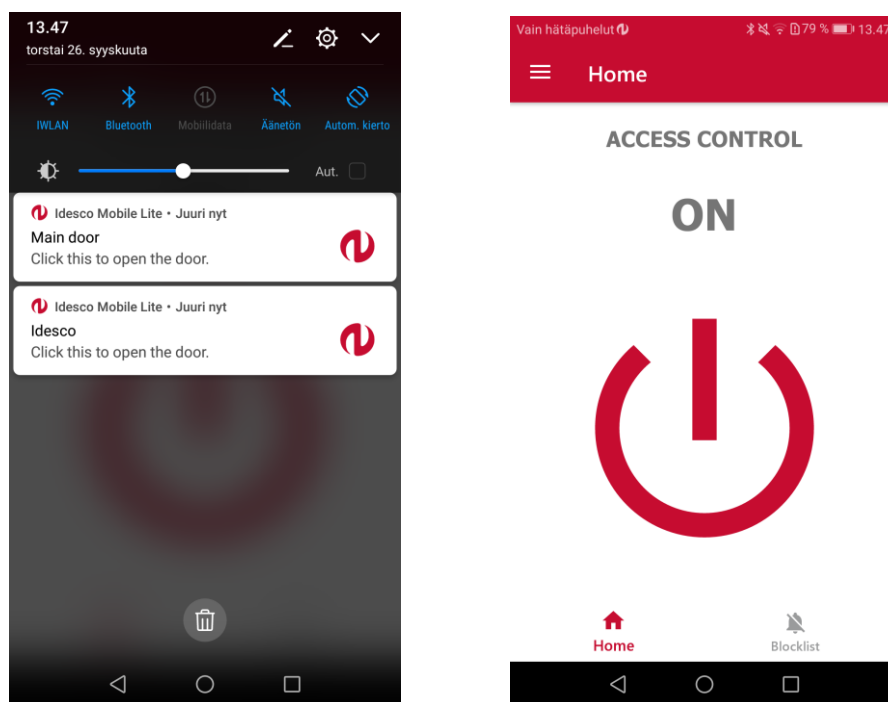
Toisessa turvallisuustasossa ovet eivät aukea automaattisesti vaan vaativat käyttäjältä näytölle ilmestyvän ilmoituksen painamista. Lähellä olevat lukijat näkyvät puhelimen käyttöjärjestelmän ilmoitusalueella joko yläpalkissa tai lukitusruudussa lukijoihin määritetyllä "friendly name"-nimellä. Tätä suositellaan oville, joita ei haluta automaattisesti avattavan, mutta avaamisen halutaan silti olevan helppoa.

Kolmas turvallisuustaso verrattuna toiseen turvallisuustasoon estää puhelimen aukaisemisen lukitusruudusta eli ovea ei voida aukaista, ellei avaa puhelimen lukitusta. Puhelimen lukituksena voi olla joko PIN-koodi, kuvio, salasana, sormenjälki tai kasvojen tunnistus. Kolmas turvallisuustaso

estää ovien aukaisemisen vääriltä käyttäjiltä. Jos käyttäjän puhelin putoaa tai joutuu väärin käsiin, on toisen käyttäjän tiedettävä alkuperäisen omistajan määrittämä puhelimen salausavain. Tämä on korkein turvataso ja sitä suositellaan esimerkiksi ulko-oville ja muille korkeamman tason salausta vaativille oville. Alkuvaiheessa toteutettu alkuperäinen kuvaus prototyypistä ja yleinen kuvaus turvatasoista löytyvät oppinnäytetyön liitteestä 2.

## 5.5 Käyttöliittymä

Käyttöliittymän suunnittelussa tähdättiin siihen, että käyttäjän painallusten määrä ja käyttöliittymään kuluva aika olisi mahdollisimman pieni. Siksi sovelluksen ulkoasussa päätettiin pyrkiä pyörittämään sovellusta Android-käyttöjärjestelmän ilmoitusten kautta. Aukaisemalla ovia yläpalkin ilmoitusten kautta, käyttäjä välttää mahdollista turhautumista esimerkiksi sovelluksen hakemisessa Androidin sovellusvalikosta. Ylimääräisiä listoja vältetään ja löydetyt ovet voidaan avata suoraan ylävalikon tai jopa lukitusruudun ilmoituksista (kuva 12).

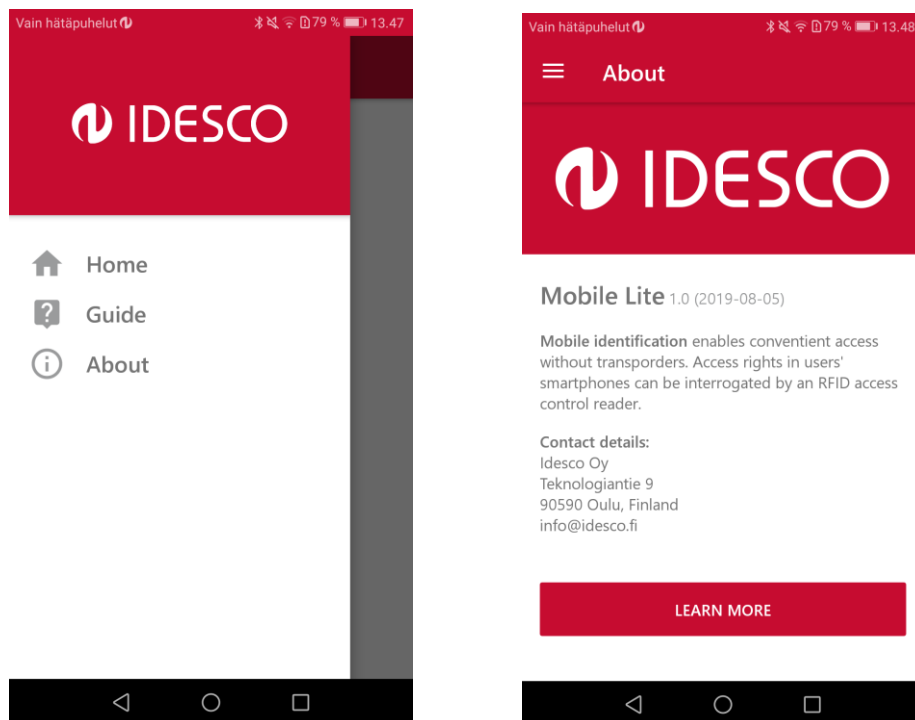


KUVA 12. Idesco Mobile Liten kustomoidut ilmoitukset ja etusivu

Pääsivu sisältää ison käynnistämisen napin (kuva 12), jonka jälkeen sovelluksen voi sulkea kokonaan ja sovellus toimii taustalla ilmoittaen ovista yläpalkin ilmoituksissa. Ilmoitusten esto-ominaisuutta myös mietittiin, missä vapaasti valittavien lähellä olevien lukijoiden esiintyminen sovelluksessa



voidaan estää. Tämä ominaisuus päätettiin jättää tulevaan versioon. Käynnistäessä sovellus ilmoittaa myös mahdollisen Bluetooth-yhteyden tai sijainnin puuttumisesta. Tilanteessa, jossa lähellä olevia ovia on monta, Android-käyttöjärjestelmä ryhmittää ylimääräiset ilmoitukset sovelluskohtaisiin ryhmiin. Käyttöliittymästä oli tarkoitus tehdä kaksi hieman eroavaa versiota ja pitää käytettävyysskysely kahden version kesken, mutta ratkaisusta tulikin varsin yksinkertainen eikä kyselyä nähty tarpeelliseksi. Idesco Mobile Liten käyttöliittymän sivuvalikon ja infosivun näkee kuvassa 13.



KUVA 13. Toteutetun käyttöliittymän kuvakaappauksia

## 5.6 Kommunikointi

Kommunikointiin sovelluksen ja lukijan välillä käytetään Bluetooth Low Energy -teknologiaa. Bluetooth-yhteyden ensimmäinen versio julkaistiin vuonna 1999. Bluetoothin lähetysetäisyys on pidempi kuin NFC-yhteys ja lyhyempi kuin WiFi-yhteys, yleensä noin 10 metriä. Tavallinen Bluetooth-yhteys lähettää koko ajan dataa, minkä takia se käyttää paljon virtaa. Sitä varten kehitettiin Bluetooth Low Energy, joka julkaistiin Bluetooth 4.0 -version yhteydessä vuonna 2010. Tässä uudessa versiossa Bluetoothilla lähetetään dataa vain, kun laitteella on jotain lähetettävää.

BLE-yhteyden data on tallennettu hierarkisesti BLE-laitteen GATT-profiiliin. Korkeimpana yksikkönä GATT-profilissa on Servicet, joiden alta löytyy Characteristicseja, jotka voivat sisältää talletettavaa dataa. Characteristic on pienin käytettävä yksikkö Bluetooth-yhteydessä ja niitä käytetään luku- ja kirjoituskomennolla. Characteristicsien käytössä laitteiden ei tarvitse tehdä paritusta vaan ne voidaan yhdistää suoraan GATT-profiiliin, kun lukijan mainostama MAC-osoite on löytynyt. Itse Bluetoothin toteutukseen käytettiin apuna avoimen lähdekoodin Bluetooth LE -kirjastoa. (52.)

Bluetooth LE -kirjasto nopeutti kehittämistä, mutta myöhemmin huomattiin, että kirjasto aiheutti välillä virheitä, kuten jättämällä ”haamuyhteyksiä” lukijoihin Bluetooth-yhteyksien sulkemisen jälkeenkin. Tähän ainoana korjauksena nähtiin olevan Bluetooth-kommunikoinnin toteuttaminen natiivikielillä, minkä toteuttaminen projektin aikataululla ei olisi ollut enää järkevää.

## **5.7 Salaus**

Mobiilisovelluksen ja lukijan välinen kommunikointi on salattu 128-bittisellä AES-salauksella. Salauksen ja kommunikointisekvenssin suunnittelijana oli Paula Koistinen, jonka suunnitelman sekä yhteistyön pohjalta toteutin yhteyden lukijaan mobiilisovelluksessa. Kaikki Bluetooth-yhteydellä lähetettävät tiedot ovat kryptattuna. Itse salausavaimen siirto lukijaan käy lukijoiden konfiguraatiokortilla.

## **5.8 Kehitysympäristö**

Toteutuksen alussa oli päättämättä, millä kehitysympäristöllä lähdemme kehittämään mobiilisovellusta. Tutkimatta oli myös, mitkä ympäristöt sallivat sovelluksen vapaan myymisen tai mitkä ovat hinnaltaan tähän ratkaisuun sopivia. Android Studio oli ensimmäinen vaihtoehto kehitysympäristöksi alkupuolella, mutta jo ennestään käytössä olleen Visual Studion alustariippumattoman Xamarin-mobiilikehitysympäristön löydyttyä, päädyimme testaamaan Xamarin-kehitysympäristöä. Tästä heräsikin kysymys, voiko tällä korkeamman tason kehitysympäristöllä päästä tarpeeksi hyvin Android-puhelimen rautaan, että voimme toteuttaa tämän hyvin Androidin käyttöjärjestelmää hyväksi käyttävän ratkaisun. Hetken tutkimisen ja sovellustestien jälkeen päädyttiin käyttämään Visual Studion Xamarin kehitysympäristöä.

Toinen syy, miksi Visual Studio Xamarin mobiilik kehitysympäristöä päädyttiin käyttämään, oli että yrityksen työntekijät olivat jo ennestään tottuneet käyttämään C#-ohjelmointikieltä. Siten olisi myös mahdollista jakaa myöhempää jatkokehitystä muillekin työntekijöille. Xamarinissa käytettiin Xamarin Formsia eli alustariippumatonta puolta, jolla voidaan luoda mobiilisovellus samaan aikaan sekä Androidille että myös iOS:lle.

Xamarinin opettelu oli alussa hidasta, mutta myös ihan luonnollista ottaen huomioon uuden kehitysympäristön. Kehitysympäristön tekniikoiden opettelun jälkeen kehitys tuntui kuitenkin hyvinkin helpolta ja luonnolliselta. Ongelmana Xamarinin opettelussa oli kuitenkin se, että ei ollut tiedossa suoraan kokeneita Xamarinin käyttäjiä, joten ainoa keino opetella Xamarinin käyttöä oli omatoimisesti. Vaikka Xamarin on melko korkean tason kehitysympäristö ja käyttää korkean tason ohjelmointikieltä, on sillä hyvin mahdollista päästä Xamarinin Forms-tasolta Android-puolelle laitetason ominaisuuksiin kiinni erityisesti DependencyService- ja MessagingCenter-tekniikoiden avulla. Esimerkiksi hyvänä esimerkkinä yläpalkin ilmoitusten toteuttaminen oli kyllä yksinkertaista, mutta hyvin rajoitettua, joten loin täysin manuaalisesti luodut ilmoitukset Android-puolella XML-kielillä DependencyServicen avulla.

C#-kieli on ollut jo ennestään Idescolla käytössä ja tulee myös pysymään pääkielenä PC-puolen sovelluksissa ja työkaluissa. C#-ohjelmointikielen harjoittelua kerkesinkin jo tekemään aikaisemmassa Idescon yrityslähtöisessä projektissa, joten Xamarin-kehitysympäristöllä ohjelmointi oli luontevaa, varsinkin taustatoimintojen toteutuksessa.

Xamarinin käyttöliittymien toteuttamiseen käytetään XAML-kieltä, joka muistuttaa hyvin paljon Android Studiossa käytettävää XML-merkintäkieltä, mutta Xamarinissa on myös mahdollista tehdä sovelluksia suoraan Androidille käyttämällä Androidin käyttöliittymätoteuttamista ja C#-taustakoodia. Kehitys aloitettiin alussa Xamarinin Android-puolella, mutta Xamarin Formsin luontevuuden ja iOS-tuen myötä vaihdoimme kuitenkin Formsiin. Tämä päätös päätyi olemaan hyödyllinen. Xamarin Formsiin oli myös laajasti saatavilla dokumentointia ja ohjeita.

Korkeamman tason ohjelmistokieli on myös huomattavasti tehokkaampi vaihtoehto pienille tai yksittäisen tekijän tiimeille kuin matalamman tason ohjelmistokielet. Korkeamman tason ohjelmointikielillä tietenkin tulee kysymyksenä teho- ja muiden resurssien käyttö, mutta näin kevyenä sovellusratkaisuna C# on oikein oiva ratkaisu. Lopullinen testattu akun kulutus oli loppujen

lopuksi pieni, 1–3 % päivässä, taustalla ollessa ja ovia aukaistessa. Kehitystä nopeutti myös erityisesti oikeiden puhelimien käyttö emulaattorin sijaan, mikä on kyllä suositeltavaa.

Xamarinilla sovellusten kehittäminen on nopeaa ja luontevaa. Myös Xamarinissa käytettävä C#-ohjelmointikieli on 96-prosenttisesti uudelleenkäytettävissä (53). Koodista noin kolme neljäsosaa on myös jo valmiiksi käytettävänä tulevassa iOS-sovelluksen toteutuksessa. Android Studiolla toteutettu sovellus olisi antanut lisänopeutta itse sovellukseen, mutta toteutus olisi ollut huomattavasti hitaampaa ja sovelluksen nopeutta ei tässä tilanteessa nähty tarpeelliseksi. Hyvin käyttöliittymärikkaille sovelluksille, joissa mobiilisovelluksen ei ole tarkoitus näyttää natiivilta, on suositeltavaa käyttää esimerkiksi Web-ohjelmointikieltä käyttäviä alustariippumattomia kehitysympäristöjä, kuten React Nativea. Jos sovelluksen keveys on myös tärkeä, Qt:n kehitysympäristö on hyvä vaihtoehto.

## 5.9 Käytettyjä tekniikoita

### 5.9.1 DependencyService

DependencyService on luokka, jolla sovelluksen on mahdollista herättää natiiviympäristön toiminnallisuuksia jaetusta ympäristöstä. DependencyServicessä luodaan rajapinta jaetussa ympäristössä ja toteutus rekisteröidään rajapinnalle natiiviympäristössä. Natiiviympäristön toteutus on sitten vapaasti kutsuttavissa rajapinnan kautta. DependencyServicen rajapintaa kutsutaan kuvan 14 kaltaisella komennolla. (54.)

```
DependencyService.Get<IDependencyService>().GetLocationState();
```

KUVA 14. Esimerkki DependencyServicen rajapintakutsusta

### 5.9.2 MessagingCenter

MessagingCenter on julkaisija-tilaajarakenteinen viestittelytekniikka, jolla voidaan lähettää viestejä ohjelmakoodin osien välillä. Julkaisu ja tilaus tehdään yhteisen merkkijonon perusteella. Julkaisijan ei tarvitse olla tietoinen vastaanottajan tai vastaanottajien olemassaolosta. Kun merkkijono on molemmilla sama, tulevat viesti ja sen sisältämät parametrit perille. MessagingCenter on

alustariippumaton, joten sitä voidaan käyttää sekä Android- että iOS-puolella. MessagingCenterin julkaisu ja tilaus hoituu kuvan 15 tavalla. (55.)

```
MessagingCenter.Send(Application.Current, ..  
    MessagingCenterEvent.StartBleService);  
  
MessagingCenter.Subscribe<Xamarin.Forms.Application>(  
    this, MessagingCenterEvent.StartBleService, message =>  
    {
```

KUVA 15. Esimerkki MessagingCenterin julkaisusta ja tilauksesta

### 5.9.3 Foreground service

Foreground service on taustalla toimiva palvelu, josta käyttäjän täytyy olla tietoinen toimiakseen. Foreground servicen luonti vaatii Androidin yläpalkin ilmoituksen, jota Android tulee näyttämään koko palvelun elinkaaren ajan. (56.)

## 6 POHDINTA

Opinnäytetyön lähtökohtana oli toteuttaa Idesco Oy:lle uusi mobiilitunnistetta hyödyntävä ratkaisu kulunvalvontaan. Tarkoituksena oli luoda mahdollisimman käyttäjäystävällinen ratkaisu mobiilitunnisteen käyttöönottamiseen kulunvalvonnassa. Alustan tarkoitus ei ollut myöskään käyttää ulkoista tietokantaa tai pilvää toimiakseen.

Työ aloitettiin suunnittelemalla mahdollista ratkaisua ja esitutkimalla markkinoilla olevia ratkaisuja. Toteutuksen käyttöympäristöksi päädyttiin ottamaan Microsoftin Visual Studiossa oleva mobiilikehitysympäristö Xamarin. Xamarinissa käytetään korkean tason ohjelmointikieltä C#:a ja projektin pääkohteena on puhelimen Android-käyttöjärjestelmä. Laajentaminen iOS-käyttöjärjestelmiin oli myös tarkoituksena myöhemmin, mikä on myös hyvin mahdollista Xamarin-kehitysympäristöllä. Ratkaisussa käytetään Bluetooth Low Energy -tekniikkaa lukijoiden ja mobiilisovelluksen välisessä kommunikoinnissa. Lopuksi luotu mobiilisovellus toteutettiin toimimaan Idesco Oy:n lukijoiden kanssa. Lukijoiden laiteohjelman muutokset eivät kuuluneet opinnäytetyöhön. Ohjelmoinnin aikaista omaa testausta suoritettiin jatkuvasti, mutta lopullisen sovelluksen testauksen hoitivat Idescon testaajat.

Projektin toteutukseen annettiin alusta asti hyvin vapaat kädet ja työn tuloksena saatiin helppokäyttöinen ja hyödyllinen kokonaisuus, jonka avulla Idesco Oy:n kulunvalvontaa saatiin laajennettua käyttämään myös älypuhelimia etätunnistimena ilman internet-yhteyttä. Omatoimisesta vapaa-ajan sovelluskehitysharrastuksesta oli hyötyä projektin etenemisessä. Idescon aikaisemmista projekteista sekä koulun Windows-mobiilikehityskursseilta tuttu C#-ohjelmointikieli tuntui luonnolliselta käyttää projektin aikana. Tuotteen kommunikoinnin salaukseen kokemusta löytyi aikaisemman toisen yrityksen yrityslähtöisen projektin toteutuksesta sekä koulun matematiikkakurssin salausalgoritmien tutkimusraportin tekemisestä.

Projektin aikaisissa välitarkistuksissa oltiin tyytyväisiä, mihin tuote oli kehittymässä. Vaikka sovelluksen ulkoasussa pyrittiin yksinkertaisuuteen, taustatoimintojen ohjelmointia tuli odotettua enemmän. Resurssien ja ajan puuttumisen takia esimerkiksi virrankulutuksen esitutkimukseen ei keretty käyttää aikaa, minkä riskinä olisi ollut, että sovellus olisi voinut viedä enemmän virtaa, kuin käyttäjät olisivat halunneet.

Projektin vapaus, vastuullisuus ja aikaisemmat vapaa-ajan harrastukset mahdollistivat luovuuden tuotteen suunnittelussa, toteutumisessa ja onnistumisessa. Suunnitellusta mobiilitunnisteesta tuli hyvä välimuoto turvallisuuden ja käytettävyyden välillä sekä se on myös helposti laajennettavissa tulevaisuudessa. Tuote lopulta päätyi asiakkaille asti Suomeen sekä ulkomaillekin (kuva 16). Suunnitellusta tuotteesta tuli helppokäyttöinen ja ainutlaatuinen ja se on herättänyt kiinnostusta monissa asiakkaissa Idesco Oy:tä kohtaan. Myöhemmin ratkaisulle yritettiin hakea myös patenttia. Idesco Mobile Lite voitti Suomen Turvallisuus & Riskienhallinta -lehden vuoden 2020 OHTO eli Oikein Hyvä Turvallisuuden Oivallus -palkinnon.



KUVA 16. Idesco Mobile Lite -mainos Slovakiassa

## LÄHTEET

1. Jokamies 2019. Kuinka älypuhelin on muuttanut arkeamme. Hakupäivä 20.5.2019. <https://www.jokamies.fi/kuinka-alypuhelin-on-muuttanut-arkeamme/>.
2. Kielitoimiston sanakirja 2020. Kulunvalvonta. Hakupäivä 21.10.2021. <https://www.kielitoimistonsanakirja.fi/#/kulunvalvonta>.
3. Evifin 2020. Tunnistautuminen. Hakupäivä 27.10.2020. <https://www.evifin.fi/tunnistautuminen/>.
4. Idesco 2019. RFID:n perusteet. Hakupäivä 21.10.2021. [https://prezi.com/2ejpf48lw4t2/rfidn-perusteet/?token=b3b38ea61896e0f1cacb40e3b9d34fc645c13b43bf71b307163763f9d63ebc4a&utm\\_campaign=share&utm\\_medium=copy](https://prezi.com/2ejpf48lw4t2/rfidn-perusteet/?token=b3b38ea61896e0f1cacb40e3b9d34fc645c13b43bf71b307163763f9d63ebc4a&utm_campaign=share&utm_medium=copy).
5. Kaleva 2017. HS: Älypuhelimien pin-koodi voidaan päätellä puhelimen asentoantureiden avulla. Hakupäivä 21.10.2021. <https://www.kaleva.fi/hs-alypuhelimien-pin-koodi-voidaan-paatella-puhelim/1870206>.
6. Idesco 2019. 8 CD 2.0 MI. Hakupäivä 21.10.2021. <https://idesco.fi/product/bluetooth-nfc-rfid-reader/>.
7. Riffid 2020. Mikä RFID? Hakupäivä 21.10.2021. <http://www.riffid.fi/mika-rfid>.
8. Idesco 2016. 125-kHz-Low-Frequency-Tags.png. Hakupäivä 21.10.2021. <https://idesco.fi/wp-content/uploads/2016/10/125-kHz-Low-Frequency-Tags.png>.
9. Keränen, Timo 2017. Sormenjäljet ja kasvokuvat yleistyvät tunnistamisessa vaaranmerkeistä huolimatta – "En käytä ennen kuin on pakko". Yle. Hakupäivä 21.10.2021. <https://yle.fi/uutiset/3-9561075>.
10. Evifin 2020. Biometrinen. Hakupäivä 3.10.2020. <https://shop.evifin.fi/Biometrinen>.



11. Pirhonen, Anna-Liisa 2007. 3d-kasvojentunnistus poimii hämäret tyypit. Tekniikka&Talous. Hakupäivä 21.10.2021. <https://www.tekniikkatalous.fi/uutiset/3d-kasvojentunnistus-poimii-hamarat-tyypit/912f2245-f71c-3088-8871-a246ca6ae6d1>.
12. Aukia, Janne 2005. Biometrinen tunnistus. Tivi. Hakupäivä 21.10.2021. <https://www.tivi.fi/uutiset/biometrinen-tunnistus/5ce9a543-967a-32cd-a3e4-5a420d667d71>.
13. Uotila, Mirva 2018. Biometrinen tunnistautuminen tekee maksamisesta turvallisempaa ja helpompaa. QVIK. Hakupäivä 21.10.2021. <https://qvik.com/news/biometrinen-tunnistautuminen-maksaminen-turvallisuus/>.
14. Hallituksen esitys 2009. Hallituksen esitys Eduskunnalle laiksi passilain ja eräiden siihen liittyvien lakien muuttamisesta 234/2008. Finlex. Hakupäivä 21.10.2021. <https://www.finlex.fi/fi/esitykset/he/2008/20080234>.
15. Konttinen, Erno 2018. Qualcomm julkisti ultraääneen perustuvan sormenjälkilukijan – tulossa uusien Samsung-huippupuhelinten näytön alle. Mobiili.fi. Hakupäivä 21.10.2021. <https://mobiili.fi/2018/12/05/qualcomm-julkisti-ultraaaneen-perustuvan-sormenjalkilukijan-tulossa-uusien-samsung-huippupuhelinten-nayton-alle/>.
16. Tuppi, Juha 2014. Facebookin kasvojentunnistusteknologia jo lähes ihmisen tasolla. AfterDawn. Hakupäivä 21.10.2021. [https://fin.afterdawn.com/uutiset/artikkeli.cfm/2014/03/18/facebookin\\_kasvojentunnistusteknologia\\_jo\\_lahes\\_ihmisen\\_tasolla](https://fin.afterdawn.com/uutiset/artikkeli.cfm/2014/03/18/facebookin_kasvojentunnistusteknologia_jo_lahes_ihmisen_tasolla).
17. Lehto, Martti 2019. Ihmisten tunnistaminen tehostuu - uhka yksityisyydelle? Upseeriliitto. Hakupäivä 22.9.2019. [https://www.upseeriliitto.fi/sotilasaikakauslehti/1\\_2019/ihmisten\\_tunnistaminen\\_tehostuu\\_-\\_uhka\\_yksityisyydelle](https://www.upseeriliitto.fi/sotilasaikakauslehti/1_2019/ihmisten_tunnistaminen_tehostuu_-_uhka_yksityisyydelle).
18. Korpimies, Annika 2015. Iiristunnistus tulee kännykkään: "Vaikea väärentää". Tivi. Hakupäivä 21.10.2021. <https://www.tivi.fi/uutiset/iiristunnistus-tulee-kannykkaan-vaikea-vaarentaa/b1096f86-4c27-3bce-aa99-cba562a4a1ac>.

19. Heikkilä, Mari 2012. Silmän iiriskin muuttuu ikääntyessä – biometrinen tunnistus voi epäonnistua. Tekniikka&Talous. Hakupäivä 21.10.2021. <https://www.tekniikkatalous.fi/uutiset/silman-iiriskin-muuttuu-ikaantyessa-biometrinen-tunnistus-voi-epaonnistua/b4203671-cd33-3ba6-a3a5-86cda72a5f2c>.
20. Tilastokeskus 2020. Liitetaulukko 13. Matkapuhelimen käyttö ja internetin käyttö televisiolla 2020, %-osuus väestöstä. Hakupäivä 4.11.2021. [https://www.stat.fi/til/sutivi/2020/sutivi\\_2020\\_2020-11-10\\_tau\\_013.fi.html](https://www.stat.fi/til/sutivi/2020/sutivi_2020_2020-11-10_tau_013.fi.html).
21. Tilastokeskus 2017. Väestön tieto- ja viestintätekniikan käyttö. Hakupäivä 21.10.2021. [https://www.stat.fi/til/sutivi/2017/13/sutivi\\_2017\\_13\\_2017-11-22\\_kat\\_002.fi.html](https://www.stat.fi/til/sutivi/2017/13/sutivi_2017_13_2017-11-22_kat_002.fi.html).
22. OP Kassa 2020. Kuusi ohittamatonta syytä käyttää mobiililaitetta kassana. Hakupäivä 4.2.2020. <https://www.op-kassa.fi/kauppiaaksi/mobiili-kassajajestelma>.
23. Haavisto, Päivi 2018. Uuden polven älyvaatteet odottavat isoa harppausta. Työhyvinvoinnin erikoislehti. Hakupäivä 21.10.2021. <https://www.ttllehti.fi/uuden-polven-alyvaatteet-odottavat-isoa-harppausta/>.
24. Laitila, Teemu 2018. Kannattaako ostaa älykello vai aktiivisuusranneke? Mieti nämä etukäteen. Talouselämä. Hakupäivä 21.10.2021. <https://www.talouselama.fi/uutiset/kannattaako-ostaa-alykello-vai-aktiivisuusranneke-mieti-nama-etukateen/90fc7bb1-56af-3f67-87ab-570a34d2ab5a>.
25. Morgun, Ivan 2017. How to get Unique ID to identify Android devices. Hakupäivä 21.10.2021. <https://en.proft.me/2017/06/13/how-get-unique-id-identify-android-devices/>.
26. Mysochenko, Yuriy 2018. How to change ANDROID\_ID on Android 8+ (Oreo) with ROOT. Medium. Hakupäivä 21.10.2021. <https://medium.com/@sdex/how-to-change-android-id-on-oreo-with-root-a71ebbc38cec>.
27. Mediapuhelin 2021. Android-puhelimen roottaus. Hakupäivä 11.11.2021. <http://mediapuhelin.net/android-puhelimen-roottaus/>.

28. Hogben, Giles 2017. Changes to Device Identifiers in Android O. Android Developers Blog. Hakupäivä 21.10.2021. <https://android-developers.googleblog.com/2017/04/changes-to-device-identifiers-in.html>.
29. Arch 2020. How To Change the MAC Address on your Android Device. Techjunkie. Hakupäivä 21.10.2021. <https://www.techjunkie.com/change-mac-address-android/>.
30. Doud, Adam 2019. How to Find Your Android Device's Serial Number. How-To Geek. Hakupäivä 21.10.2021. <https://www.howtogeek.com/414617/how-to-find-your-android-devices-serial-number/>.
31. hackinganonymous 2016. How to Change Serial Number of Your Phone!!!!. Hakupäivä 21.10.2021. <https://hackinganonymous.wordpress.com/2016/12/14/how-to-change-serial-number-of-your-phone/>.
32. Google 2021. Mainokset. Play Console Ohjeet. Hakupäivä 18.12.2019. [https://play.google.com/about/monetization-ads/ads/#!?zippy\\_activeEl=ad-id#ad-id](https://play.google.com/about/monetization-ads/ads/#!?zippy_activeEl=ad-id#ad-id).
33. Firebase 2020. FirebaseInstanceId. Google Developers. Hakupäivä 18.12.2019. <https://firebase.google.com/docs/reference/android/com/google/firebase/iid/FirebaseInstanceId>.
34. Android Developers 2021. Best practices for unique identifiers. Google Developers. Hakupäivä 21.10.2021. <https://developer.android.com/training/articles/user-data-ids>.
35. HID Global 2021. About HID Global. Hakupäivä 21.10.2021. <https://www.hidglobal.com/about>.
36. HID Global 2021. HID Mobile Access Solutions. Hakupäivä 21.10.2021. <https://www.hidglobal.com/solutions/hid-mobile-access-solutions>.
37. ePressi 2017. Bitwards esittelee uuden digitaalisen alustan laitteiden yhteiskäyttöön. Hakupäivä 21.10.2021. <https://www.epressi.com/tiedotteet/suunnittelu-ja-teknikka/bitwards-esittelee-uuden-digitaalisen-alustan-laitteiden-yhteiskayttoon.html>.

38. Bitwards 2021. Mobile ID. Hakupäivä 21.10.2021. <https://www.bitwards.fi/mobile-id/>.
39. Bitwards 2021. Bitwards. Google Play. Hakupäivä 21.10.2021. <https://play.google.com/store/apps/details?id=fi.bitwards.bitwardskeyapp&hl=fi>.
40. LenelS2 2021. Company Overview. Hakupäivä 21.10.2021. <https://www.lenel.com/about/company-overview>.
41. LenelS2 2021. BlueDiamond™ Readers and Mobile Credentials. Hakupäivä 21.10.2021. <https://www.lenel.com/products/bluediamond>.
42. LenelS2 2021. Lenel Enhances BlueDiamond™ Platform, Announces Pathways Feature. Hakupäivä 21.10.2021. <https://www.lenel.com/news-events/lenel-enhances-bluediamond-platform-announces-pathways-feature>.
43. STid 2021. Our vision. Hakupäivä 21.10.2021. <https://stid-security.com/en/business/about-stid>.
44. STid 2019. STid Mobile ID. Hakupäivä 4.12.2019. [https://stid-security.com/images/private-pdf/Flyer\\_STid\\_Mobile\\_ID\\_V5\\_US.pdf](https://stid-security.com/images/private-pdf/Flyer_STid_Mobile_ID_V5_US.pdf).
45. Nedap 2021. History. Hakupäivä 21.10.2021. <https://nedap.com/about-us/history/>.
46. Nedap 2021. Merchandise Simply Available. Hakupäivä 21.10.2021. <https://www.nedap-retail.com/>.
47. Nedap 2021. MACE READER MM (QR). Hakupäivä 21.10.2021. <https://portal.nedapidentification.com/download/MACE/Datasheet/English/MACE%20Reader%20MM%20QR%20datasheet>.
48. AR Media 2019. Nedap to launch MACE at ifsec1. Hakupäivä 4.12.2019. [https://www.securityworldmarket.com/int/News/Product-News/nedap-to-launch-mace-at-ifsec1#.Xee\\_W3tS9aQ](https://www.securityworldmarket.com/int/News/Product-News/nedap-to-launch-mace-at-ifsec1#.Xee_W3tS9aQ).

49. AMAG Technology 2021. About us. LinkedIn. Hakupäivä 21.10.2021. <https://www.linkedin.com/company/amag-technology>.
50. AMAG Technology 2019. Symmetry Blue. Hakupäivä 21.10.2021. [https://5b393dae-7185-4776-bec2-756ed3cf4652.filesusr.com/ugd/ad4185\\_21bc6ed730f347a6972f7bbf050b20f2.pdf](https://5b393dae-7185-4776-bec2-756ed3cf4652.filesusr.com/ugd/ad4185_21bc6ed730f347a6972f7bbf050b20f2.pdf).
51. AMAG Technology 2021. Symmetry Blue. Hakupäivä 21.10.2021. <https://www.amag.com/blue>.
52. CrossComm, Inc. 2019. Building Android Apps to Control Bluetooth LE Devices. Youtube. Hakupäivä 21.10.2021. <https://www.youtube.com/watch?v=zeN88yh7YdY>.
53. Cogan, Adam 2015. Getting 96% Code Reuse with Xamarin Forms. Hakupäivä 21.10.2021. <https://adamcogan.com/2015/01/14/getting-96-code-reuse-with-xamarin-forms/>.
54. Microsoft 2021. Xamarin.Forms DependencyService Introduction. Hakupäivä 21.10.2021. <https://docs.microsoft.com/en-us/xamarin/xamarin-forms/app-fundamentals/dependency-service/introduction>.
55. Microsoft 2021. Xamarin.Forms MessagingCenter. Hakupäivä 21.10.2021. <https://docs.microsoft.com/en-us/xamarin/xamarin-forms/app-fundamentals/messaging-center>.
56. Microsoft 2021. Foreground Services. Hakupäivä 21.10.2021. <https://docs.microsoft.com/en-us/xamarin/android/app-fundamentals/services/foreground-services>.

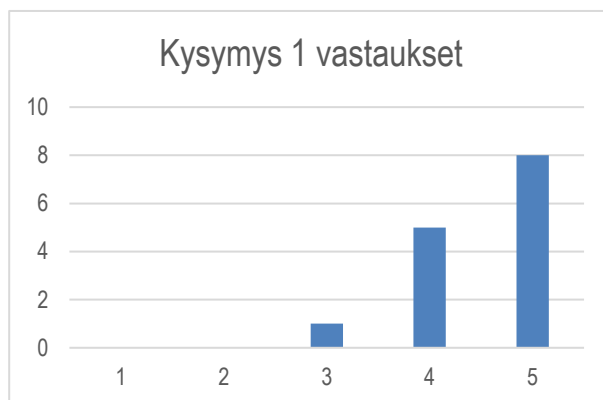
**1. Kuinka tärkeänä näet, että puhelinsovellus kuluttaa mahdollisimman vähän akun tehoja.**

Ei väliä

Erittäin tärkeä

☐☐☐☐☐

Kommentteja:

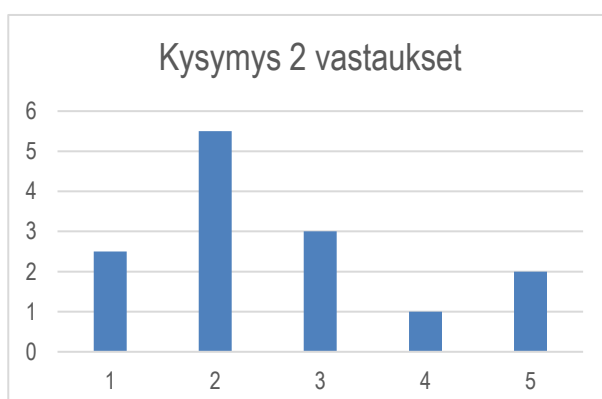
Keskiarvo:  
4,5**2. Häiritseekö sinua, että työpaikan järjestelmä keräisi työntekijän huomaamatta logia työntekijöiden liikkumisesta rakennuksessa?**

Ei häiritse

Häiritsee paljon

☐☐☐☐☐

Kommentteja:

Keskiarvo:  
2,607143

3. Kuinka hyvin luottaisit älypuhelimien toimivuuteen tänä päivänä?

En luota ollenkaan

Luottaisin täysin

☐ ☐ ☐ ☐ ☐

Kommentteja:



Keskiarvo:  
3,714286

4. Mikä on maksimi viive oven aukaisuun, mitä jaksaisit odottaa painettuasi puhelinsovelluksen "avaa ovi"-nappia?

Väh. 0,5s 1s 2s 3s 4s 5s

☐ ☐ ☐ ☐ ☐ ☐ ☐

Kommentteja:



Keskiarvo:  
3,928571

**5. Kuinka tärkeänä näet puhelimen NFC ominaisuuden myös yhtenä aukaisukeinona (puhelin lukijaa vasten oven aukaisuun)?**

Ei tarvitse

Erittäin tärkeä

☐☐☐☐☐

Kommentteja:



Keskiarvo:  
3,571429





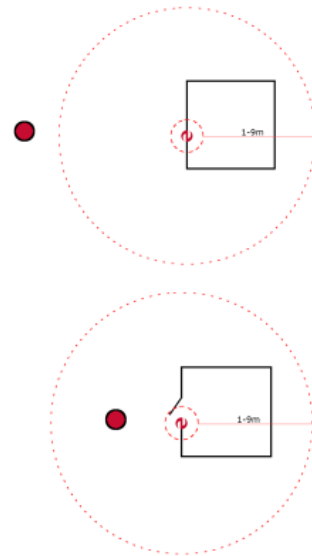
## Yleistä

- Projektin ideana on ottaa älypuhelin käyttöön kulunvalvonnassa
- BLE lite sisältää kolme eri turvatasoa
- Turvatasot voidaan määritellä ovi- ja käyttäjäkohtaisesti järjestelmästä
- Ohjelma käyttää mahdollisimman vähän virtaa ja toimii taustalla ilman sovelluksen avaamista
- Ei vaadi verkkoyhteyttä



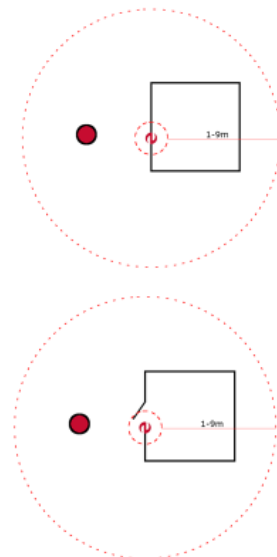
## Turvataso 1 (Sisäoville)

- Heikoin turvallisuustaso
- Puhelimeen ei tarvitse koskea (voi olla taskussa)
- Etäisyys voidaan määritellä ovikohtaisesti järjestelmästä / konfiguroimalla



## Turvataso 2

- Ovet eivät aukea automaattisesti vaan vaaditaan oven mainostuksen painaminen puhelimen lukitusruudusta
- Oven avaaminen ei vaadi puhelimen lukituksen avaamista
- Jos lukitusruudussa ei ole painanut ovea, löytyvät ovet myös aloitusruudun yläpalkin ilmoituksista
- Max 5 lähintä ovea listattuna lähimmästä kauimpaan



## Turvataso 3

- Oven aukaisuun vaaditaan puhelimeen määritellyn suojauksen avaaminen
- Salauksena voidaan käyttää puhelimen tarjoamia salausmenetelmiä
  - PIN-koodi
  - Kuvio
  - Salasana
  - Sormenjäljen tunnistus
  - Kasvojen tunnistus
- Lähimpien ovien ilmoitukset näkyvät päävalikon yläpalkissa
- Lukitusruudun ilmoituksia voi myös painaa, mutta ovet avautuvat vasta lukituksen avaamisen jälkeen

