

KARELIA-AMMATTIKORKEAKOULU  
Tietojenkäsittelyn opetusohjelma

Maria Zudina

NFC-TEKNOLOGIA JA SEN SOVELTAMINEN

Opinnäytetyö  
Toukokuu 2017



**OPINNÄYTETYÖ**  
**Toukokuu 2017**  
**Tietojenkäsittelyn opetusohjelma**

Tikkarinne 9  
80220 JOENSUU  
013 260 600

Tekijä(t)  
Maria Zudina

Nimeke  
NFC-teknologia ja sen soveltaminen

Toimeksiantaja  
Karelia-ammattikorkeakoulu

#### Tiivistelmä

Työn tarkoitus on perehtyä Near Field Communicationsin eli NFC:n toimintaperiaatteisiin ja hyödyntää teknologiaa käytännön applikaation luomisessa. Työssä mietitään myös NFC-teknologian nykyisiä sekä potentiaalisia käyttökohteita. Työn toimeksiantona oli tutkia NFC-teknologian soveltumista luokkahuoneiden varausjärjestelmään ja miettiä mahdollisia muita ratkaisuja varausjärjestelmän modernisointiin.

Tutkimusmenetelmänä opinnäytetyössä käytettiin vertailevaa ja empiiristä tutkimusta. Työn tieto-osuus käsittelee teknologian teoreettista puolta vertailevan tutkimuksen muodossa ja empiirisen tutkimuksen aineistoksi kehitettiin NFC-teknologiaa hyödyntävä sovellus Android-älypuhelimille. Työn tulokset saatiin sekä vertailemalla NFC-teknologiaa muihin etätunnistustekniikan vaihtoehtoihin että testaamalla teknologian käyttömukavuutta käytännön sovelluksen avulla.

Työssä käy ilmi, että NFC ei itsessään ole paras ratkaisu toimeksiantajan ongelmaan, vaan toimeksiantajan on mielekkäämpää joko pysyä vanhassa järjestelmässään tai hyödyntää QR-koodeja. NFC:n hyödyt QR-koodeihin verrattuna eivät osoittautuneet oleellisiksi toimeksiantajan käyttötarkoituksen kannalta.

Kieli

suomi

Sivuja 30

Liitteet 0

Asiasanat

NFC, RFID, QR, Bluetooth, Etätunnistustekniikka



**THESIS**  
**May 2017**  
**Degree Programme In Business**  
**Information Technology**

Tikkarinne 9  
80220 JOENSUU  
013 260 600

Author  
Maria Zudina

Title  
NFC-Technology and its applications

Commissioned by  
Karelia University of Applied Sciences

#### Abstract

This thesis takes a deeper look at the NFC technology and its current applications, as well as inspects the potential applications of this technology. As a part of this study a demo application is created, which uses NFC-technology. The commission for this thesis was to research if the NFC technology could be used to modernize and digitalize the classroom reservation application on Karelia UAS.

As a research method in this thesis comparative and empirical researches were used. In the theoretical part of this work comparative research is used for comparing NFC to other technologies of close range wireless communication, and the empirical research is carried out by creating and analyzing the demo application for Android mobile phones.

In this thesis it can be concluded that NFC is not the best option for the commissioner to update the classroom reservation application. For the commissioner it would be more beneficial to either keep their current system or to update to using QR-codes, which are more inexpensive and would serve the purpose in question better than NFC. The benefits of NFC technology towards QR-codes proved to be irrelevant to the commissioner's task.

Language

Finnish

Pages 30

Appendices 0

Keywords

NFC, RFID, QR, Bluetooth

## Sisältö

1	Johdanto .....	6
2	Etätunnistustekniikka.....	8
2.1	RFID .....	9
2.2	NFC .....	11
2.3	Bluetooth .....	12
2.4	QR-koodit .....	13
3	Käyttökohteet .....	14
3.1	Käyttö peleissä .....	15
3.2	Käyttö ihmisissä.....	16
4	Empiirinen tutkimus .....	17
4.1	Tutkimusongelma .....	17
4.2	Tutkimusmenetelmät ja työkalut .....	18
4.3	Teknologian soveltaminen .....	19
5	Tulokset ja yhteenveto .....	21
6	Pohdinta.....	24
	Lähteet .....	29

**Käsitteet**

NFC	Near Field Communication, lähietäisyystiedonsiirto (NFC Forum 2016).
RFID	Radio Frequency Identification, radiotaajuinen etätunnistus. (Wikipedia 2016)
Tagi	Siru tai tarra, jota hyödynnetään tekniikassa tunnistena.
ISM-taajuusalue	Maailmanlaajuinen radiotaajuuskaista, jonka käyttö ei vaadi erillistä lupaa ja joka on alun perin tarkoitettu teolliseen, tieteelliseen ja lääketieteelliseen käyttöön. (Wikipedia 2016.)

# 1 Johdanto

Aloitin aiheen tutkimisen voidakseni perehtyä itselleni uuteen teknologiaan, jota alkoi näkyä ympäristössä yhä enemmän. Huomasin NFC-teknologian käytön ensimmäisen kerran toimiessani Activisionin julkaiseman Spyro Skylanders -pelin testaajana. Pelissä käytettiin NFC-teknologiaa tiedonsiirtoon. Silloin luulin toimintaa vielä jotenkin magneettipohjaiseksi, mutta ajan kanssa törmäsin NFC-tageihin yhä enemmän.

Opinnäytetyön toimeksiantajana toimii Karelia-ammattikorkeakoulu, joka pyysi selvittämään, voiko NFC-teknologiaa hyödyntää tehostamaan koulun arkea, esimerkiksi luokkatilojen varaushallintajärjestelmän yhteydessä. Tavoitteena on korvata luokkien näkyvä varaustilanne luokkahuoneiden ulkopuolella digitaaliseen muotoon; soveltuuko NFC-teknologia tällaiseen käytännön digitalisointiin kouluympäristössä ja onko se kannattavaa?

Tässä opinnäytetyössä tutkitaan NFC-teknologiaa ja sen nykyisiä käyttökohteita sekä toteutetaan pienimuotoinen demo-ohjelma teknologian sovellukselle käytännössä. Demon on tarkoitus esitellä teknologian mahdollistamaa tiedonsiirtoa ilman internetiä älypuhelimien ja tagin välillä.

NFC-teknologia alkaa hiljalleen levitä yhä yleisempään käyttöön muun muassa maksukorttien muodossa, mutta peleissä se on vielä melko tuntematon. Pelialaan erikoistuneena tarkoitukseni on omaksua tämä teknologia ja miettiä sen käyttöä myös peleissä.

Opinnäytetyön tutkimusmenetelmänä on monimenetelmätutkimus. Alun teoreettisen puolen toteutan teoreettisen sekä vertailevan tutkimuksen avulla. Tavoitteena on käsitellä teknologiaa teoreettisella tasolla ja tarkastella olemassa olevaa dokumentaatiota, jonka pohjalta vertailen sitten teknologiaa muihin olemassa oleviin vaihtoehtoihin.

Työn lopussa toteutan käytännön sovelluksen empiirisen tutkimuksen aineistoksi, josta teen konkreettisia havaintoja tukemaan loppupohdintaani. Käytännön sovellus on yksinkertainen Android-puhelimille suunnattu sovellus, joka hyödyntää NFC:n mahdollistamia NFC-tagien luku- ja kirjoitusominaisuuksia. Sovelluksen avulla pyrin selvittämään, miten käyttökelpoinen tämä ohjelma olisi toimeksiantajan määrittämässä ympäristössä.

Aiempiä tutkimuksia NFC-teknologiasta löytyi hyvin suppeasti, ja valtaosa niistä käsitteli pikemminkin RFID-etätunnistusteknologiaa. Löytämäni tutkimukset olivat myös melko vanhoja, melkein kymmenen vuoden takaa. Tarkoitus onkin tällä työllä päivittää tutkimusta ajan tasalle ja verrata teknologian nykytilannetta aiempien tutkimusten ennustuksiin.

Opinnäytetyön on tarkoitus palvella kaikkia NFC-teknologiasta kiinnostuneita tahoja, jotka haluaisivat saada riittävän käsityksen teknologian toimintaperiaatteista ja mahdollisesti myös päästä alkuun tämän teknologian hyödyntämisessä omiin sovelluksiinsa. Opinnäytetyön sisällön on tarkoitus tarjota myös kattava tietopohja NFC:stä suomen kielellä, sillä olen suomentanut siihen kaikki käyttämäni lähteet. Valtaosa saatavilla olevista lähteistä tästä aiheesta on englanniksi, joten englannin kieltä osaamattomat tahot saavat tämän työn avulla vankan käsityksen aiheesta myös suomen kielellä. Käytännön sovelluksen tekoon on myös kerätty hyödyllisiä lähteitä teknologian ohjelmointiin, joten NFC-teknologian käytännön soveltamisesta kiinnostuneet tahot voivat päästä helposti alkuun lähdeluettelossa mainittujen lähteiden avulla.

## **Opinnäytetyön sisältö**

Opinnäytetyön johdannossa kerrotaan lyhyesti ydinasiat opinnäytetyön sisällöstä, käytetyistä menetelmistä, työn tarkoituksesta ja tavoitteista. Opinnäytetyössä käytetyt käsitteet on selitetty työn alussa.

Luvussa kaksi käydään läpi NFC-teknologian teoreettista puolta ja selvitetään sen toimintamenetelmiä sekä historiaa. NFC-teknologiaa verrataan myös muihin

käytössä oleviin tiedonsiirtomenetelmiin. Luvussa tarkastellaan lisäksi sitä, kuinka muita tiedonsiirtomenetelmiä hyödynnetään erikseen ja yhdessä NFC-tekniologian kanssa.

Luvussa kolme perehdytään NFC-tekniologian aiempiin ja nykyisiin käyttökohteisiin. Luvun tarkoitus on tutkia, miten tekniologiaa on sovellettu tähän mennessä ja mitä potentiaalisia tulevaisuuden käyttökohteita on vielä tulossa. Myös NFC-tekniologian käyttöä peleissä käydään läpi.

Luku neljä käsittelee opinnäytetyön käytännön osaa, joka on empiirisen tutkimuksen pohja. Siinä kuvataan opinnäytetyöhön kuuluvan käytännön sovelluksen tekoprosessia ja sen aikana kohdattuja haasteita sekä niihin löytyneitä ratkaisuja.

Luvussa viisi kerrotaan ja käsitellään opinnäytetyön tuloksia. Selvitetään, soveltuuko tekniologia toimeksiannon tehtävään vai ei, sekä esitetään mahdollisia vaihtoehtoratkaisuja opitun pohjalta. Tekniologian soveltuvuutta mietitään myös muihin käyttökohteisiin, joita ei aikaisemmin vielä käsitelty, ja pohditaan tekniologian yleistä tulevaisuutta.

Työn lopussa pohdintaosuudessa arvioidaan opinnäytetyön tuloksia sekä käsitellään työtä prosessina. Luvussa kerrotaan kohdatuista haasteista sekä niiden ratkaisusta, puidaan työn kulkua ja sen onnistumista. Lisäksi pohditaan valittujen työ- ja tutkimustapojen soveltuvuutta sekä opinnäytetyön hyödyllisyyttä ja luotettavuutta.

## **2 Etätunnistustekniikka**

Etätunnistustekniikka on nimensä mukaisesti tekniologia, joka mahdollistaa langattoman tunnistuksen kahden laitteen välille. Etätunnistustekniikkaa esiintyy sekä radiotaajuuksien että skannausten muodossa, jotka kummatkin ovat yleisessä käytössä muun muassa kaupoissa. (Wikipedia 2016.) Tässä



opinnäytetyössä keskitytään radiotaajuuden avulla tapahtuvaan etätunnistukseen ja viivakoodeja sekä muita etätunnistuksen keinoja ei käsitellä.

## 2.1 RFID

RFID on lyhenne sanoista Radio Field Identification. Se tarkoittaa radiotaajuuden avulla tapahtuvaa etätunnistusta. RFID on etäluvun ja -tallentamisen menetelmä, jossa käytetään RFID-tageja tai -tunnisteita. RFID-tunniste tai toisin sanottuna saattomuisti on pienikokoinen laite, joka voidaan sisällyttää tuotteeseen valmistusvaiheessa tai liimata kiinni siihen jälkikäteen tarran muodossa. Eläimiin tunniste voidaan lisätä sirun muodossa injektoimalla se ihon alle tai kiinnittämällä se korvalapulla. RFID-tunnisteet sisältävät pienen antennin voidakseen lähettää ja vastaanottaa radiotaajuisia kyselyitä RFID-lähetin-vastaanottimelta. (Wikipedia 2016; RFID Lab Finland Ry 2017a.)

RFID-yhteys saadaan aikaan, kun sekä tagissa että lukijassa olevat antennit saavat yhteyden toisiinsa. Antennien pienen koon takia yhteyden on muodostuttava tarpeeksi pienellä etäisyydellä. Lukija muuntaa silloin sirulta saamansa radiosignaalin digitaaliseen muotoon, joka voidaan välittää edelleen tietokoneelle tai muulle lukijalaitteelle käsiteltäväksi. (Wikipedia 2016.)

RFID-lukijalla on kolme tehtävää: tuottaa sähkömagneettisella kentällään passiiviselle tai puolipassiiviselle tunnisteelle tiedon lähettämiseen tarvittava energia, ottaa vastaan tunnisteiden lähettämä tieto ja prosessoida se. Lukuetaisyyden määrittää sekä lukijan että tunnisteiden antennien koko ja lukijan lähettämän sähkömagneettisen kentän voimakkuus. Vaikka lukijaa kutsutaankin lukijaksi, voi se myös muuttaa, lisätä tai poistaa sähkömagneettisen kenttensä avulla tunnisteella olevaa tietoa, mikäli tunnisteiden muistiominaisuus sen sallii. (Wikipedia 2016.)

RFID-tunnisteet voivat olla joko aktiivisia, passiivisia tai puolipassiivisia. Passiivisilla RFID-tunnisteilla ei ole omaa virtalähdettä, vaan laitteen aktivoitumiseen vaadittava erittäin pieni sähkövirta muodostuu antenniin

saapuvasta radiotaajuisesta skannauksesta, jonka avulla tunniste pystyy lähettämään vastauksen lukijalaitteelle. Virta- ja hintavaatimuksista johtuen passiivisen RFID-tunnisteen vastaus on lyhyt, tyypillisesti vain ID-numero. Oman virtalähteen puuttuminen tekee laitteesta varsin pienen. Passiivisten tunnisteiden lukuetaisyydet vaihtelevat 10 mm:n ja 5 metrin välillä. (Wikipedia 2016; Sunsero 2017; Thrasher 2013.)

Puolipassiivinen RFID-tunniste sisältää virtalähteen, mutta ei omaa lähetintä. Omalla virtalähteellä saavutetaan kuitenkin passiivista tunnistetta suurempi toimintasäde ja mahdollistetaan laajennettu toiminnallisuus, mukaan lukien tietojen säilyttäminen tunnisteen omassa muistissa. (Wikipedia 2016; Sunsero 2017.)

Aktiiviset RFID-tunnisteet puolestaan sisältävät virtalähteen ja niillä voi olla pidempi kantomatkä sekä suurempi muisti kuin passiivisilla tunnisteilla. Ne voivat myös tallentaa lähetin-vastaanottimen lähettämiä lisätietoja. Tällä hetkellä pienimmät aktiiviset RFID-tunnisteet ovat suunnilleen kolikon kokoisia, mutta ohuempia. Monilla aktiivisilla tunnisteilla lukuetaisyydet ovat kymmeniä metrejä ja pariston ikä useita vuosia. (Wikipedia 2016; Sunsero 2017.)

Koska passiiviset tunnisteet ovat huomattavasti aktiivisia tunnisteita halvempia valmistaa, on suurin osa tällä hetkellä käytettävistä RFID-tunnisteista passiivisia. Vuonna 2004 passiivisen tunnisteen hinta oli n. 0,25 €. Tavoitteena oli saada tunnisteiden hinnat n. 0,05 euroon, jotta RFID-tekniikasta tulisi kannattavaa ja laajasti käytettyä. (Wikipedia 2016.)

Nykyään käytetään yleisesti neljänlaisia RFID-tunnisteita, jotka eroavat toisistaan käytetyn radiotaajuuden perusteella: matalan taajuuden tunnisteet (125–134 kHz), korkean taajuuden tunnisteet (13,56 MHz), UHF-tunnisteet (868–956 MHz) ja mikroaaltotunnisteet (2,45 GHz). Näistä ainoastaan taajuus 2,45 GHz on käytettävissä kansainvälisesti, sillä se on vapaasti hyödynnettävällä ISM-taajuusalueella. (Wikipedia 2016.)

## 2.2 NFC

NFC on lyhenne sanoista Near Field Communication. NFC on yksi radiotaajuista etätunnistustekniikkaa (RFID) käyttävistä teknologioista. Suurin ero NFC:n ja RFID-tekniikan välillä on, että NFC-laite voi toimia samanaikaisesti sekä lukijalaitteena että tunnisteena, toisin kuin perinteiset RFID-laitteet. (Faulkner 2015; Thrasher 2013.)

NFC-yhteys perustuu sähkömagneettiseen induktioon radiotaajuudella 13,56 MHz. Tiedonsiirtonopeus voi olla 106, 212 tai 424 kbit/s, jotka soveltuvat pienten tietomäärien siirtoon. Suurempia tietomääriä käsiteltäessä NFC:tä voi käyttää avaamaan yhteys, jossa varsinainen tiedonsiirto hoidetaan esimerkiksi Bluetoothilla. NFC-yhteys toimii parhaiten alle 10 cm:n säteellä, mutta teoriassa 20 cm:iin asti. (Wikipedia 2017a; Thrasher 2013.)

NFC-protokollan mukaisessa kommunikaatiossa on aina kaksi osapuolta. Osapuolet ovat niin sanottu aloitteentekijä sekä kohde. Aloitteentekijä käynnistää tiedonsiirron, minkä lisäksi se vastaa kommunikoinnista koko tiedonsiirron ajan. Kohde sen sijaan toimii passiivisena osapuolena vastaten aloitteentekijältä saamiinsa pyyntöihin. Kun toisella yhteyden muodostavista laitteista on yhteys internettiin, myös toinen voi vaihtaa dataa online-palvelujen kanssa. Tyypillisesti passiivisina osapuolina NFC-yhteydessä ovat NFC-tagit. (Wikipedia 2017a; Thrasher 2013.)

NFC-tagit ovat passiivisia tietosäiliöitä, joita voidaan lukea ja ylikirjoittaa aktiivisen NFC-laitteen avulla. NFC-tagit ovat tyypillisesti kooltaan 96 - 8,192 bittiä ja voivat olla joko avoimesti kaikkien luettavissa, tai ne voi olla koodattu erikseen salausalgoritmeilla tiedon suojaamiseksi rajattuun käyttöön. Suojattuja tietotyyppejä voivat esimerkiksi olla pankkikortin tiedot tai PIN-numerot. (Wikipedia 2017a.)

Jokainen aktiivinen NFC-laite voi toimia kolmessa eri muodossa:

- NFC-korttiemulaattori: Mahdollistaa laitteen toimimisen NFC-korttina, antaen käyttäjien suorittaa rahallisia tapahtumia, kuten suorittaa maksuja tai käyttää laitetta pääsylippuna.
- NFC-lukija/kirjoittaja: Antaa laitteen lukea ulkopuolisiin NFC-tarroihin kirjattuja tietoja tai muokata niitä. Tarrat voivat olla esimerkiksi julisteessa.
- NFC peer-to-peer: Mahdollistaa kahden NFC-laitteen kommunikation keskenään paikallista tiedonsiirtoa varten.

NFC-standardeista vastaa NFC Foorumi, joka on ollut myös vastuussa teknologian mainostamisesta ja levittämisestä. Foorumi määrittää myös neljä eri tyyppiä NFC-tageille, jotka tarjoavat eri tiedonsiirtonopeuksia ja mahdollisuuksia muun muassa muokkaukseen, salaukseen ja uudelleenkirjaukseen. (Wikipedia 2017a.)

NFC:n tiedonsiirto itsessään ei ole salattua, vaikka sen toimintasäde onkin hyvin pieni. Tämän takia tiedonsiirto on haavoittuvainen välikäsien tiedonmuokkaukselle. Tietyt sovellukset voivat tarjota omaa salausta, esimerkiksi SSL-salausta, turvatakseen tiedonsiirron. Vuonna 2015 NFC Foorumi julkaisikin Signature Record Type Definition -määritelmän (RTD), joka antaa NFC-laitteelle oikeuden tarkistaa tagin tiedot ja nähdä sen luojan tiedot. (NFC Forum 2015.)

### **2.3 Bluetooth**

Bluetooth on avoin standardi laitteiden langattomaan kommunikointiin lähietäisyydellä. Bluetooth käyttää tiedonsiirtoonsa ISM-radiotaajuuksia väliltä 2400 - 2480 MHz, luoden niiden avulla henkilökohtaisia paikallisia tietoverkkoja, joilla on varsin hyvä tietosuoja. Teknologia on alun perin kehitetty korvaamaan RS-232-datakaapeleita. Bluetooth mahdollistaa useamman laitteen samanaikaisen yhteyden, eikä siinä ole synkronointiongelmia. (Absolute Astronomy 2016.)

Sekä NFC että Bluetooth ovat lyhyen kantaman johdottomia tiedonsiirtomenetelmiä, jotka ovat myös matkapuhelinten käytössä. NFC:n

tiedonsiirto on Bluetoothia hitaampaa, mutta käyttää huomattavasti vähemmän energiaa ja muodostaa yhteyden paljon nopeammin, sillä se muodostuu automaattisesti, ilman erillistä laitteen tunnistusta. NFC-yhteys voidaan luoda vain yhteen vastakappaleeseen kerrallaan automaattisen tunnistuksen takia, mutta Bluetooth-laite voi ylläpitää yhteyttä samanaikaisesti jopa seitsemän eri laitteen kanssa. (Absolute Astronomy 2016.)

Ero on myös toimintaetäisyydessä, sillä NFC:n kantama on vain noin 10 cm, jolloin yhteys on huomattavasti turvallisempi. Bluetoothin kantama on pitempi ja aktiiviset laitteet näkyvät kauas ja yhteys on paljon helpompi korruptoida. Kahta teknologiaa käytetään yleensä rinnakkain, niin että molempien hyödyt saadaan maksimoitua. Yksi tällainen käyttötapa käyttää NFC-teknologiaa avaamaan yhteyden kahden laitteen välille, ettei manuaaliin yhdeydenluomiseen olisi tarvetta. Yhteyden muodostuttua itse tiedonsiirto toteutuu nopeampaa tiedonsiirtoa hyödyntävällä Bluetoothilla. (Wikipedia 2017a.)

## **2.4 QR-koodit**

QR-koodit ovat Quick Response -koodeja, jotka toimivat skannattavina linkkeinä. QR-koodit ovat mustien ja valkoisten neliöiden muodostama kuva, jota skannaamalla laite ohjautuu QR-koodin määräämään kohteeseen. Näitä kohteita voivat olla esimerkiksi nettisivu, sähköposti, puhelinnumero tai teksti.

(What is a QR Code? 2017)

QR-koodeja voi lukea käyttämällä ohjelmia, jotka tukevat niiden skannauksen. Skannaus tapahtuu tyypillisesti kameraa käyttäen ja skannauslaitteina ovatkin tyypillisesti älypuhelimet tai kannettavat pelilaitteet. Sekä skannaus- että QR-koodien generaattoriohjelmat ovat kummatkin saatavilla älypuhelimille. (What is a QR Code? 2017)

QR-koodit ovat tällä hetkellä erittäin suuressa suosiossa Aasiassa ja varsinkin Japanissa, mutta alkavat yleistyä myös muualla. QR-koodien yleisyys ja suosio selittyy niiden helppoudella, sillä niiden levittäminen vaatii tosiaankin vain yhden

neliönmuotoisen kuvan, joka voi olla sijoitettuna mille pinnalle tahansa. Kunhan kuvan kontrasti on tarpeeksi suuri mustien ja vaaleiden kohtien välillä, skannaus pystyy lukemaan sen ja ohjaamaan koodin mukaiseen kohteeseen. (What is a QR Code? 2017)

QR-koodi on käytännössä hyvin samanlainen kuin viivakoodi. Sen suurin ero on siinä, että se on kahdensuuntainen, ja käyttää siis viivojen sijaan neliöitä. Näin koodin voi lukea kahdesta suunnasta. Perinteinen viivakoodi taas vaatii skannerilta juuri tietyn asennon toimiakseen. (What is a QR Code? 2017)

QR-koodit ovat siis täysin passiivisia, ja NFC-tageihin erotettuna eivät sisällä itsessään mitään toiminnallisuutta. Ne eivät muodosta mitään yhteyttä, vaan ovat pikemminkin kuviomuotoon kryptattu hyperlinkkipätkä, jonka skannausohjelma tulkitsee ja ohjaa sen pohjalta kohdesivustolle. Luotua koodia ei myöskään voi jälkeinpäin enää muokata, vaan jokaiselle uudelle sisällölle kehitetään vain oma, uusi koodi. (What is a QR Code? 2017)

### **3 Käyttökohteet**

NFC:tä käytetään yhä enemmän muun muassa teollisuudessa viivakoodin sijaan. NFC:n etuna on, että se ei vaadi suoraa yhteyttä lukijan ja tagin välille. Lukija voi kommunikoida tagin kanssa kahdella eri tavalla: matalilla taajuusalueilla käytetään induktiivista kytkentää ja korkeammilla taajuusalueilla käytetään sähkökenttään perustuvaa kytkentää. (Wikipedia 2016; RFID Lab Finland Ry 2017c.)

Matalan taajuuden NFC-tunnisteita käytetään yleisesti eläinten tunnistuksessa, oluttynnyrien jäljittämisessä, autojen käynnistyksen- ja varkaudenesto-järjestelmissä sekä joissakin kulunvalvontajärjestelmissä. Eläimet tunnistetaan esimerkiksi siruttamalla ne tai lisäämällä NFC-tagin karjaeläimien korvaan. Tagiin kirjataan yksilön tiedot ja omistajan yhteystiedot. Tagin avulla voidaan valvoa eläimen löytymistä pakotilanteessa tai erottaa yksilö karjalauman keskuudesta.

Teollisuudessa valmisteilla olevat tuotteet voidaan myös merkata NFC-tageilla, joille kirjataan aina, mitä kaikkia toimenpiteitä tuote on jo läpikäynyt ja mitkä on tekemättä. Näin koko tuotanto voidaan helposti koneellistaa. (Wikipedia 2016.)

Korkean taajuuden NFC-tunnisteita käytetään kirjastoissa ja kirjakaupoissa kirjojen jäljittämiseen, kuormalavojen, lentolaukkujen ja vaatteiden jäljittämiseen sekä rakennusten kulunvalvontaan. Korkeataajuiset tunnisteet ovat laajasti käytettyjä erilaisissa tunnusmerkeissä korvaamassa magneettiraitoja. Näitä tunnusmerkkejä tarvitsee vain pitää tietyn matkan päässä lukijasta, jotta tunnusteen haltija voidaan tunnistaa. NFC-tageja voidaan käyttää myös esimerkiksi avaimina elektronisiin oviin. Joissain järjestelmissä tagien käyttö korvaa myös kellokortin. (Wikipedia 2016; RFID Lab Finland Ry 2017c.)

Laitteet, joissa on NFC-ominaisuus, kuten esimerkiksi älypuhelimet, voivat käyttää erilaisia applikaatioita lukeakseen NFC-tageja tai toimiakseen maksupäätteenä toiseen sopivaan NFC-päätteeseen. NFC-yhteyden kautta kaksi laitetta voidaan yhdistää turvallisesti, minkä jälkeen voidaan siirtää suurempi määrä dataa esimerkiksi Bluetooth-yhteyttä käyttäen. Älypuhelimet ovat myös suosituin NFC-lukijatyyppejä, sillä niillä on yhtä helppoa lukea NFC-tageja kuin esimerkiksi QR-koodeja. Toinen yleinen käyttö ovat Bluetooth-kuulokkeet, jotka aktivoidaan NFC:n avulla. (Tech Radar 2015; RFID Lab Finland Ry 2017b.)

Maksukorteissa NFC-muotoista tiedonsiirtoa käytetään maksukortin ja maksutermiinin välisessä kontaktittomassa tiedonsiirrossa. Tällöin kyse on VISA- tai MasterCard-maksamisesta pankin tai muun kortin myöntäjän maksukortin avulla. Maksutapaa kutsutaan lähimaksuksi. (Tech Radar 2015; RFID Lab Finland Ry 2017c.)

### **3.1 Käyttö peleissä**

Peleissä NFC-teknologian käyttö näkyi ensimmäisenä Skylanders: Spyro's Adventure -pelissä, jossa pelihahmot olivat fyysisiä figuureja, joihin oli upotettu NFC-tagit. Kun figuuri tuotiin pelin lukijalaitteelle, hahmon tiedot siirtyivät peliin, ja

näin tietoa voitiin siirtää pelistä toiseen figuurin mukana. Figuuriin tallennettiin muun muassa pelihahmon tiedot sekä voima, joten figuuri toimi ikään kuin liikkuvana, pelistä ja pelikoneesta irrallisena tallennustiedostona. (Tech Radar 2015; RFID Lab Finland Ry 2017b.)

Nykyään Nintendo on laajentanut NFC-tagien käyttöä entisestään Amiibo-figuurien avulla, jotka ovat samanlaisia NFC-tagitettuja figuureja kuin Skylanders-pelissä. Myös kaikki Nintendon uusimmat konsolit sisältävät NFC-lukijan ominaisuudet. Muut peliyhtiöt eivät ole vielä ottaneet teknologiaa yhtä laajamittaisesti käyttöönsä, mutta joitakin mobiilisovelluksia on jo olemassa, joissa peleihin siirretään dataa fyysisten keräilykorttien avulla, joissa kaikissa on NFC-tagit. (Wikipedia 2017b.)

### **3.2 Käyttö ihmisissä**

Alun perin eläimille suunniteltuja ihon alle istutettavia RFID-siruja on istutettu myös ihmisiin. Siruilla voidaan valvoa pääsyä muun muassa rakennuksiin, tietokoneelle tai potilastietoihin ja jopa pyrkiä ehkäisemään kidnappauksia. Kehon tilaa tarkkaileviin antureihin yhdistettynä tunnisteella voidaan tarkkailla potilaiden tilaa. Eräs barcelonalainen yökerho käyttää ihon alle istutettavia RFID-siruja VIP-asiakkaidensa tunnistamiseen, jotta he voivat maksaa tunnisteiden välityksellä juomansa. (Wikipedia 2016.)

Méxicon kaupungin poliisilaitos on istuttanut n. 170 poliisilleen Verichip-tunnisteen mahdollistaakseen heille pääsyn poliisin tietokantoihin. Tunnisteen ajateltiin olevan hyödyksi myös kidnappaustilanteissa, auttamaan jäljittämään poliiseja. Yhdysvalloissa on joissakin osavaltioissa asennettu vangeille rannekellon kokoisia lähettimiä, jotka havaitsevat, mikäli vanki yrittää poistaa lähettimen. Tällöin lähetin lähettää hälytyksensä vankilan tietokonejärjestelmälle. (Wikipedia 2016.)



## 4 Empiirinen tutkimus

Tässä luvussa keskitytään opinnäytetyön käytännön osuuden eli empiirisen tutkimuksen toteutukseen. Empiirisessä tutkimuksessa tutkimustulokset saadaan tekemällä konkreettisia havaintoja tutkimuskohteesta ja analysoimalla ja mittaamalla sitä. Empiirisessä tutkimuksessa konkreettinen ja koottu tutkimusaineisto on tutkimuksen keskiössä ja toimii tutkimuksen tekemisen lähtökohtana. (Jyväskylän Yliopisto 2014.)

Tämän työn empiirisen tutkimuksen aineistona on itse toteutettu käytännön sovellus. Sovellus on soveltuva Android-älypuhelimille ja sen on tarkoitus hyödyntää NFC-teknologiaa ja mahdollistaa älypuhelimien toimimisen lukijalaitteena. Sovelluksen avulla puhelin voi olla vuorovaikutuksissa NFC-tagien kanssa lukemalla niitä ja kirjoittamalla niihin käyttäjän haluamia viestejä.

### 4.1 Tutkimusongelma

Toimeksiannon puolesta tutkimusongelmana oli selvittää, soveltuuko NFC-teknologian käyttö ammattikorkeakoulun kouluympäristöön korvaamaan nykyisin käytössä olevaa luokkatilojen varausmenetelmää. Tutkimustulosten pohjalta on tarkoituksena pohtia myös muita mahdollisia ratkaisuja järjestelmän päivittämiseksi.

Henkilökohtainen tavoitteeni on oppia käyttämään NFC-teknologiaa eri sovelluksissa ja perehtyä sen toimintalogiikkaan. Päämääränä on pystyä tämän jälkeen toteuttamaan uusia sovelluksia itse ja hyödyntämään teknologiaa mahdollisimman monipuolisissa käyttökohteissa. Työn avulla haen myös apua uusien mahdollisten käyttökohteiden ideointiin tulevaisuutta varten.

## 4.2 Tutkimusmenetelmät ja työkalut

Käytännön osuudessa luotiin demo-sovellus, jossa hyödynnettiin opinnäytetyön tietoperustaa. Sovellusta on käytetty empiirisen tutkimuksen lähdemateriaalina, ja sen pohjalta ratkaistiin toimeksiannon tutkimusongelma.

Valitsin juuri nämä menetelmät siksi, että voisin lähestyä tutkimusongelmaa sekä teoriapuolelta, hyödyntämällä aiemmin tehtyjä tutkimuksia aiheesta, että tarkistamalla teknologian käytön mielekkyyttä ja helppoutta käytännön toteutuksen muodossa. En halunnut pohjustaa tutkimustulostani pelkkään teoriaan, vaan halusin pystyä esittämään käytännössä, miksi saamani tulos joko soveltuu tai ei sovellu toimeksiannon pyyntöön. Monimuototutkimus on tämän takia mielestäni tähän tutkimusongelmaan soveltuvin ja perusteellisin lähestymiskeino.

Käytännön toteutuksen työkaluina käytin Android Studiota, fyysisiä NFC-tageja sekä omaa Android-puhelintani. Valitsin kehitysympäristöksi Android Studio -ohjelman siksi, että minulla on ollut siitä aiempaa kokemusta, ja olen luonut sillä joitakin mobiiliapplikaatioita koulun kursseille. NFC-tagit sekä lukijalaitteena toimiva puhelin ovat taas välttämättömiä työkaluja teknologian testaamiseen, sillä ilman niitä ohjelman toimivuutta olisi mahdotonta tarkistaa.

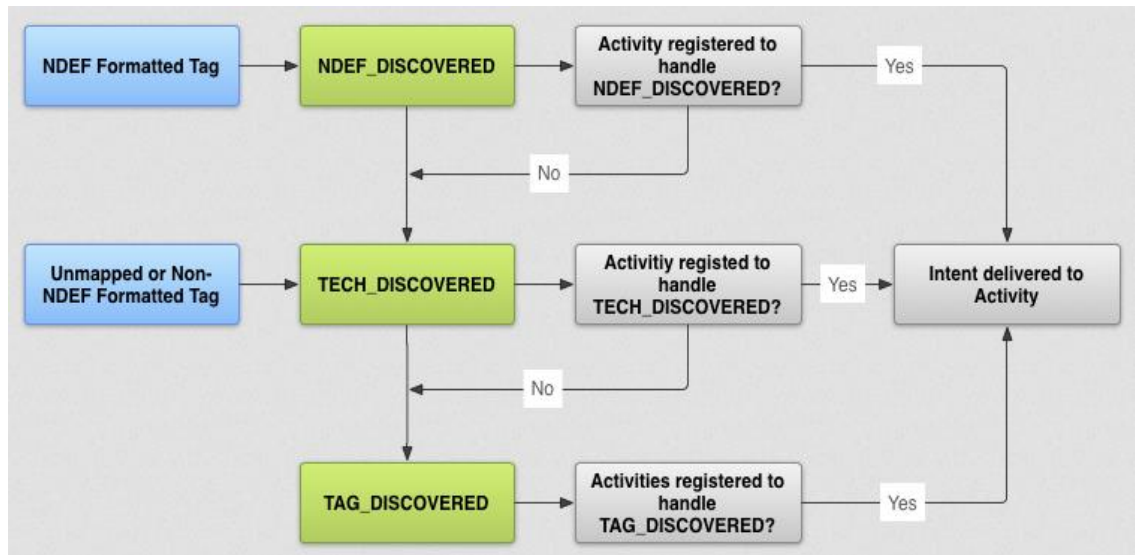
En suorittanut erillistä testiympäristöä sovellukseni perusteelliseen testaukseen, vaan suoritin sen toiminnan kotona. En nähnyt syytä viedä tageja ja älypuhelinta oikeaan koulurakennukseen tarkistaakseni sen toimivuutta siellä, sillä käytännön osuuden rajaukseni oli vain perustoiminnallisuuden toteuttaminen, eikä viimeistellyn, asiakkaille suunnatun tuotteen kehittäminen. Testasin ohjelman toimivuutta useampaan eri tagiin ja kahdella eri puhelimella varmistuakseni sen riittävästä vakaudesta.

### 4.3 Teknologian soveltaminen

Perehdyin ensin NFC-tekniikan perusteisiin teorian kautta, minkä jälkeen siirryin yksinkertaiseen Ralf Wondratschekin (2013a) kirjoittamaan NFC-tagin lukuohjelman malliesimerkkiin, jonka löysin internetistä. Perusteet selvisivät esimerkin avulla melko hyvin, mutta vastaan tuli ongelmana se, että kaikki tagini olivat tyhjinä, ja niiden lukeminen oli mahdotonta. Sain ohjelmasta kuitenkin pohjan siihen, miten ohjelma tunnistaa tagin olemassaolon.

Seuraavaksi etsin toisen Framentos Developersien (2013) malliesimerkin, jossa neuvottiin, miten tiedon kirjoittaminen NFC-tagiin onnistuu. Sen kanssa itselleni tuli ongelmia siinä, etten voinut oikein tarkistaa, menikö syöttämäni viesti tagiin asti vai ei. Malliesimerkistä nimittäin puuttui tällä kertaa tagien lukuominaisuus. Yritin nyt yhdistää näiden kahden malliesimerkin toiminnallisuudet yhteen sovellukseen, jotta voisin varmistua kummankin toiminnasta. Lopulta sain tulokseksi yhtenäisen ohjelman, joka suoritti sekä luku- että kirjoitustoiminnot. Tähän auttoi Codexpedian (2017) ohjeet.

NFC-ohjelman perustana on ensin tekniikan tunnistaminen koodissa. Tunnistamisen jälkeen voidaan ohjelmassa NFC-tekniikkaa käyttäen suorittaa tiettyjä toimintoja. Koska NFC-tageja on erilaisia ja jokaisella on omat määritelmänsä, on ohjelman luokiteltava tunnistettu tagi. Kuva 1 esittää yksinkertaisen toimintasarjan, jonka avulla ohjelma tunnistaa ja luokittelee saamansa signaalin NFC-tagista.



Kuva 1. Sekvenssikaavio (Wondratschek 2013b).

Mikäli tagi on siis NDEF-määritelmien mukainen, se tunnistetaan heti, ja tuloksena saadaan NDEF\_DISCOVERED. Mikäli tagi ei ole määritelmien mukainen, mutta sen teknologia on kuitenkin tuttu, tulokseksi tulee TECH\_DISCOVERED. Mikäli taas tagin kryptausta tai teknologiaa ei tunnisteta, ajetaan TAG\_DISCOVERED. (Codexpedia 2017.)

Viestien lukemista ja kirjoittamista varten data pitää käsitellä NDEF:n muotoon. NDEF:ssä data on kapseloitu viestiin, “NdefMessage”, joka sisältää yhden tai useamman “NdefRecord”-elementin. Kaikki viestit lukijalaitteen ja tagin välillä pitää siis formatoida näiden kahden elementin mukaiseen muotoon. (Codexpedia 2017.)

Kun lukijalaite skannaa NFC-tagin, jossa on jo jotain NDEF-formatoitua dataa, se muuntaa viestin lukukelpoiseksi ja yrittää tulkita tagin sisältämän datan MIME-tyyppiä tai URI-identifikaatiota. Tämän se tekee lukemalla NdefMessage ensimmäisen NdefRecordin päätelläkseen, kuinka tulkita koko NDEF-viestin. (Codexpedia 2017.)

## 5 Tulokset ja yhteenveto

NFC-tekniikan käytön hahmotus osoittautui käytännössä hieman vaikeammaksi kuin oletin. Tekniikan irralliset osat näyttivät hyvin selkeitä, mutta lopulta eri toimintojen yhdistäminen käytännössä tarvitsi paljon perusteellisempaa perehtymistä ja tutkimista. Varsinkin viestien parsimistarpeet tarvitsevat toimiakseen hyvin tarkkaa syntaksia, jossa pienikin virhe aiheutti lukuhäiriöitä. Lopulta kuitenkin selvisi, että NFC-aplikaatiolta ei vaadita paljoa toiminnallisuutta, jotta sillä voi luoda hyödyllisiä sovelluksia, sillä sen ydintehtävä on kuitenkin vain muodostaa yhteyksiä NFC-tageihin.

Luomani demo mahdollistaa siis NFC-tagien lukemisen ja kirjoittamisen, ja sen avulla voikin jo jättää viestejä tageihin muiden luettavaksi. Normaali NFC-lukijalla varustettu laite, kuten esimerkiksi älypuhelin, toimii automaattisesti lukijalaitteena, mutta ilman kirjoitusominaisuutta.

Näin ollen esimerkiksi minun demoani voisi käyttää tietynlaisena admin-ohjelmana. Opettaja voisi esimerkiksi sen avulla jättää viestin luokkahuoneen läheisyyteen laitettuun tagiin, että tunnit pidetäänkin jossain toisessa luokassa, tai että hän palaa kello kolme takaisin, ja opiskelijat voivat sitten omilla kännyköillään lukea viestin tagista, ilman mitään tarvetta asentaa omiin puhelimiinsa ylimääräisiä ohjelmia.

Toimeksiannon mukaisen luokkavarausjärjestelmän luominen ei kuitenkaan tätä tekniikkaa käyttäen onnistu, sillä tagien tietosäiliömäärä on hyvin rajallinen, eivätkä ne riitä ylläpitämään monimutkaista ja jatkuvasti päivittyvää varausjärjestelmää. Luomani demo-aplikaatio myös ylikirjaa aina edellisen tagin sisältämän viestin, joten senkään puolesta en pysty suosittelemaan tätä tekniikkaa käytettäväksi suuren organisaation varausjärjestelmien ylläpitoon.

Tällä hetkellä en näe yhdenkään RFID-tekniikan vielä haastavan perinteistä paperin ja kynän yhdistelmää luokkahuoneen kyljessä ratkaisemaan luokkavarausten tilanteen. Jos tekniikkaa kuitenkin halutaan hyödyntää,

ehdotan linkin jättämistä, joka veisi lukijan suoraan internetissä päivitettävään varausjärjestelmäohjelmaan. Tähän soveltuvat sekä QR-koodit että NFC-tagit, mutta ne pakottavat samalla lukijan käyttämään internet-dataa lukijalaitteessaan. Kustannustehokkaampi ratkaisu toimeksiannon ongelmaan olisivat kieltämättä QR-koodit, sillä toisin kuin NFC-tagit, niiden kustannus on vain paperi, jolle ne tulostetaan.

Itse varausjärjestelmä pitää siis ylläpitää normaalina verkkosovelluksena, johon vain päästään kätevämmiin käsiin skannauslinkin kautta, kuin käsin osoitteen näppäilemällä. QR-koodeihin voidaan toki liittää kunkin huoneen ID, joka ohjaa varausjärjestelmän oikealle sivulle. Verkkosovelluksen tietokannat ylläpitävät varaustilannetta, joskin ID:iden mahdollisesti muuttuessa on muistettava päivittää myös koodit.

Suurin hyöty NFC-tagien käytössä esimerkiksi QR-koodeihin on mielestäni se, että niiden käyttö ei tarvitse lainkaan internet-yhteyttä. QR-koodit yleensä vain ohjaavat käyttäjän jollekin internet-sivulle ja laukaisevat puhelimen selaimen, mutta jos käyttäjällä on esimerkiksi maksullinen internet tai ei verkkoa lainkaan, hän ei saa haluamaansa tietoa helposti. NFC-tagit taas toimivat ilman mitään verkkoa, ja puhelimesta ei tarvitse olla edes sim-korttia sisällä, kun kaikki viestintä tapahtuu nimenomaan radioaaltoaajuuksilla lukijan ja tagin välillä.

Koska toimeksiantoani ei kuitenkaan voi suorittaa ilman kunnollista verkkosovellusta, internet-yhteys on välttämätön. Tämän takia NFC menettää tässä suhteessa suurimman etuutensa QR-koodeihin nähden, ja näin ollen suosittelenkin nimenomaan QR-koodeja toimeksiannon ongelman ratkaisuun kustannustehokkaampana ratkaisuna.

Suosisin NFC-tageja käytettäväksi mieluummin esimerkiksi museoissa, joissa lisätieto taideteoksista voidaan kirjoittaa NFC-tagisiin. Turisteilla varsinkin on hyvin harvoin 3G-verkkoa kohdemaassa, eikä museoissakaan ole aina vapaata langatonta verkkoa saatavilla. Olen nähnyt joidenkin taidemuseoiden hyödyntävän QR-koodeja tässä suhteessa, mutta niiden korvaaminen NFC-tageilla olisi mielestäni huomattavasti toimivampaa.

Kulttuurin käyttökohteet eivät toki rajoitu pelkästään museoihin, sillä myös muut turisteille suunnatut nähtävyydet voidaan merkitä NFC-tageilla. Kaupungin patsaat, eläintarhojen tietotaulut tai mitkä tahansa muut lisätietoja tarvitsevat kohteet olisivat toimivia kohteita NFC:n hyödyntämiseen. Tagi pitää vain sijoittaa esimerkiksi lasipinnan taakse, jotta se ei kärsisi säästä ja merkitä sen sijainti näyttävästi, sillä tagi itsessään on melko pieni ja huomaamaton. Varsinkin katukuvassa tällaiset tagit jäävät potentiaalisilta käyttäjiltään huomaamatta, ellei niiden olemassaoloa esitetä näyttävästi.

Kolmas sopiva NFC-tagien käyttökohde olisi GeoCaching-tyylinen teknologian pelillistäminen, jossa tageja piilotellaan eri paikkoihin, ja niiden löytäjät voivat merkata löytäneensä ne ja jättää niihin omia viestejään. Tällä hetkellä kyseisessä pelissä on tyypillisesti käytössä vain pienet ympäriinsä piilotetut muistilehtiöt, joihin löytäjät merkkavat löytönsä käsin.

NFC-tageja voisi piilotella ympäristöön helpommin ja niiden piilopaikat voisivat olla jopa selvästi näkyvissä. Tagien pienen koon ja tarramaisen rakenteen takia toimivana piilopaikkana voi toimia jopa satunnainen juliste seinällä. Potentiaalisten piilopaikkojen lisääntyessä myös peli itsessään saisi paljon enemmän sisältöä ja enemmän haastetta. Joukolla tagitettuja kortteja voi myös toteuttaa erilaisia seurapelejä vaikkapa kaveriporukalleen, kun jokaiseen tagiin kirjoittaa palasen arvoitusta, ja pelaajien tehtävänä olisi löytää kaikki kortit ja koostaa niiden tiedoista ratkaisun pelin arvoitukseen.

Toteutettu demoni on hyvin yksinkertainen, mutta soveltuu käyttökelpoiseksi pohjaksi vaativampiinkin sovelluksiin, käyttökohteesta riippuen. Siihen voitaisiin lisätä esimerkiksi aikaleimaominaisuus, jossa jätetty viesti olisi aikaleimattu. Näin viestin lukija voisi heti nähdä, milloin viesti oli jätetty. Yksi lisättävä ominaisuus voisi myös olla edellisten viestien säilyttäminen, jolloin eri tageja lukiessa edellisten tagien viestit jäisivät ohjelman muistiin. Uniikin allekirjoituksen lisääminen jokaiseen kirjoitettuun viestiin auttaisi myös tekemään viesteistä luotettavampia, ja jonkinlainen tietosuoja on ehdoton vaatimus laajempaan käyttöön.

Jo nykyisellä toiminnallisuudella ohjelma on käyttökelpoinen moneen NFC-käyttökohteeseen, sillä oletuksena kaikkiin puhelimiin tulee vain lukuominaisuus, eikä kirjoitusmahdollisuutta. Ohjelman varsinainen kaupallinen tai laajamittainen käyttöönotto vaatii kuitenkin jonkinlaisen tietosuojauksen asentamista, sillä tällä hetkellä se on täysin avoin. Näin kuka tahansa, joka asentaa puhelimeensa jonkun toisen NFC-kirjoitustoiminnolla varustetun ohjelman esimerkiksi Playstoresta, voi halutessaan ylikirjoittaa tageihin jätetyt viestit.

Toimeksiannon tehtävän kielteisestä tuloksesta huolimatta oma henkilökohtainen tavoite tuli tällä työllä hyvin saavutetuksi. Luomani käytännön sovelluksen ansiosta olen todistanut itselleni, että ymmärrän teknologian toimintaperusteet ja kykenen kehittämään sen ympärille toimivia sovelluksia. Minulla on tämän sovelluksen myötä nyt myös valmiina hyvä pohja, jolle voin tulevaisuudessa rakentaa jotain suurempaa.

Kokonaisuutena työn sisältö on tiivis ja asiakeskeinen paketti kaikille, jotka haluaisivat saada hyvän peruskäsityksen siitä, mikä NFC on ja lähteä itseni kaltaisesti kehittämään sen tiedon avulla omia sovelluksiaan. Luotan teoriapuolelle keräämiini lähteisiin, ja käytännön sovelluksen lähteistä olen saanut konkreettistakin tulosta, joten pidän työtä kokonaisuudessaan luotettavana.

## **6 Pohdinta**

Kokonaisuutena opinnäytetyö onnistui mielestäni hyvin vastaamaan toimeksiantoon ja henkilökohtaisiin tavoitteisiini. Vaikka toimeksiannon tehtävä ei ratkennutkaan NFC-teknologiaa hyödyttäen, siihen löytyi aiheeseen perehtyessä perusteltu toinen ratkaisuehdotus. Henkilökohtaisena tavoitteenani oli hyödyntää tätä opinnäytetyöprosessia perehtyäkseni itselleni täysin tuntemattomaan teknologiaan ja oppia käyttämään sitä. Tämän vuoksi työssä on mukana myös



empiirisen tutkimusmenetelmän käytännön osio, joka auttoi teknologian omaksumista sekä henkilökohtaisen tavoitteeni saavuttamista.

Opinnäytetyön kirjoitusprosessi oli minulle suhteellisen vaivaton ja omasta mielestäni lopputulos vastaa asetettuja vaatimuksia. Kokonaisuutena tämä raportti on mielestäni hyvä aloituspaketti NFC-teknologiaan perehtymiselle. Näen hyödylliseksi myös lähteiksi keräämäni tutoriaaliesimerkit, jotka auttavat ketä tahansa NFC-teknologian soveltamista ajattelevaa.

Opinnäytetyön valmistuminen suunnitellussa aikataulussa ei kuitenkaan onnistunut. Alun perin suunnittelin toteuttavani sen nopealla aikataululla, noin kuukauden sisällä. Se ei kuitenkaan onnistunut, sillä kohtasin käytännön sovelluksen teossa pitemmän blokin, joka tauotti itsessään opinnäytetyön tekoa yli kuukaudella.

Haasteet myös yksityiselämän osalta aiheuttivat opinnäytetyön hitaamman etenemisen, sillä toisin kuin sillä, kaikella muulla oli tarkat aikarajat. Opinnäytetyö ei kuitenkaan estänyt tutkinnon valmistumista, joten sen pystyi aina jättämään myöhemmäksi kiireellisempien asioiden edeltä. Prosessin tahaton pitkittyminen kuitenkin aiheutti minulle jonkin verran stressiä varsinkin silloin, kun se ei edennyt lainkaan yli kuukauden aikana käytännön osion takia.

Jos voisin tehdä opinnäytetyössäni jotain toisin, niin lähtisin lähestymään käytännön sovelluksen tekemistä eri kannalta. Työssä lähdin tutkimaan NFC-teknologian soveltamisen toimintamenetelmiä yksittäisten osien kautta, jotka lopulta vain aiheuttivat ongelmia, kun niiden yhdistäminen ei ollutkaan selkeää. Olisi pitänyt heti alkuun etsiä kokonaisvaltaista malliesimerkkiä, jota tutkia. En lähtenyt siihen tällä kertaa, sillä epäilin, ettei sellaista ole, vaan joutuisin tutkimaan ohjelman rakennetta erillisten internetissä esitettyjen kysymysten pohjalta.

Minun olisi myös ehkä pitänyt käyttää lähdemateriaalina enemmän muiden tekemiä opinnäytetöitä, sillä olisin ehkä oppinut niistä myös oikeanlaisen raportin rakenteen tekemisen. Löytämäni työt olivat kuitenkin kaikki varsin vanhoja, joten näin luotettavammaksi viitata jatkuvasti päivitettävään ja ajan tasalla pidettävään

Wikipediaan, jossa suunnilleen samat asiat oli esitetty päivittyneemmässä muodossa. Varsinkin teknologian osalta lukemani Wikipedian artikkelit vaikuttivat luotettavilta ja kattavilta lähteiltä kaikkeen siihen tietoon, jota tässä työssä tarvitsin.

## **Menetelmien soveltuminen**

Valitut tutkimusmenetelmät soveltuivat opinnäytetyöhön mielestäni varsin hyvin. Tutkittavaan tietoon pääsin perehtymään sekä teoriassa että käytännössä. Toisaalta, jos olisin rajannut opinnäytetyöstäni pois empiirisen tutkimuksen ja suorittanut sen pelkästään teoriapuolelta, työhön käytetty aika olisi ollut huomattavasti suppeampi. Uuden teknologian soveltaminen ohjelmoinnin muodossa on hidasta ja pitkiäkin pohdintataukoja vaativa prosessi, kun taas pelkkä materiaalin etsiminen ja sen referoiminen on varsin suoraviivaista.

Kehitystyökalujen valinta oli mielestäni myös hyvin soveltuva tarkoitukseensa, sillä Android Studion käyttö ei juurikaan aiheuttanut minulle ongelmia, kun olen perehtynyt sen käyttöön ennenkin. Mitään monimutkaista en sillä tosin toteuttanut, mutta se ei ollut tämän opinnäytetyön osalta tarkoituskaan.

## **Hyödyt**

Tästä opinnäytetyöstä hyötyvät kaikki ne, jotka haluavat lisätietoa NFC-teknologiasta ja sen käytännön mahdollisuuksista, toimeksiantajani, sekä minä itse. Huomasin tätä työtä tehdessäni, että kaikki saatavilla oleva materiaali tästä aiheesta on varsin vanhaa, joten NFC-teknologiaa ei ole käsitelty kovin paljon viime aikoina. Opinnäytetyöni tarjoaa vähän uudenlaisempaa näkemystä ja päivitystä aikaisempaan tietoon, vaikka sisältö pohjautuukin jo olemassa olevaan tietoon.

Valtaosa viittaamastani materiaalista on englanninkielisiltä sivuilta. Työni myös suomentaa keräämäni tiedon yksin kansiin niiden käyttöön, jotka eivät englannin

kieltä hallitse. Varsinkin itse NFC:stä ei löytynyt suomeksi juuri mitään, vaikka RFID oli kyllä laajemmin käsitelty suomenkielisissä lähteissä. Osa opinnäytetyössä käytetyistä termeistä olivat kyllä hyvin haastavia suomentaa.

Aiempiä aihetta käsitteleviä tutkimuksia ei löytynyt lainkaan, sillä nimenomaan NFC:hen ei kukaan tuntunut rajaavan tutkimustaan. Laajemmin RFID:istä löytyi kyllä aiempaakin tutkimusta, yksi niistä on lähteenä käytetty Tomi Salmin opinnäytetyö ”Radiotaajuinen etätunnistus” vuodelta 2007. Sekin on tosin tällä hetkellä jo kymmenen vuotta vanha työ, joka teknologian kehitystahdilla tekee siitä jo vanhentuneen.

Opinnäytetyöni tarjoaa lähteen myös kaikille heille, jotka haluaisivat hyödyntää NFC-teknologiaa ohjelmoinnin puolella ja liittää sen omiin sovelluksiinsa. Mielestäni kävin tässä työssä kaikki tarpeelliset asiat sekä teorian että käytännön puolelta, jotka mahdollistavat teknologian soveltamisen ja jatkokehittämisen itsenäisesti. Luulen, että työn avulla voidaan luoda sujuvasti pienimuotoinen NFC-applikaatio.

## **Haasteet**

Suurimpana haasteena tässä työssä ajallisesti itselleni oli toimivan demosovelluksen luominen. En ole aikaisemmin ohjelmoinut mitään etätunnistusta tai radioaaltoja hyödyntävää ohjelmaa, joten sen toimintamenetelmien omaksuminen vei minulta paljon aikaa. Olen kuitenkin tyytyväinen lopputulokseen.

Toisena haasteena minulle tuli sopivan lähdemateriaalin löytäminen opinnäytetyön teoreettiseen osuuteen. Kuten jo aiemmin mainitsin, suurin osa materiaalista on vanhentunutta. Tähän viittaa myös esimerkiksi se, että noin puolet Wikipedia-artikkeleiden käytetyistä lähteistä ovat tällä hetkellä kadonneet tai vanhentuneet. En kuitenkaan epäile Wikipedia-artikkeleiden luotettavuutta. Pidän niitä luotettavana lähteenä tämän työn tarkoituksiin.

## Tulevaisuus

Prosessina opinnäytetyö oli itselleni hyvin antoisa, ja aion jatkaa aiheen tutkimista eteenpäin sovelluskehityksen muodossa. Haluan yhdistää tämän teknologian peleihin kokonaisvaltaisemmin, kuin mitä Nintendo tekee tällä hetkellä amiibo-hahmoillaan. Haluan kehittää pelin nimenomaan NFC-tagien ympärille, eikä vain käyttää niitä työkaluna tuomaan sisältöä peliin.

Olen iloinen nähdessäni teknologian olevan yhä enemmän läsnä pelimaailmassa, ja siksi löytämäni lähdemateriaalin vanhanaikaisuus tuotti suuren yllätyksen. NFC ei ole vielä vanhentunut teknologia, mutta siihen keskittyvän tutkimuksen ja artikkeleiden määrä on vähäistä. Teknologiaa kuitenkin sovelletaan yhä näkyvämmiin ihmisten arkielämässä muun muassa mobiilimaksujen ja pankkikorttien etämaksuominaisuuksina, joten mielestäni nyt olisi juuri sovelias aika muidenkin avata silmänsä ja keskittyä tähän teknologiaan tarkemmin.

Toivottavasti opinnäytetyöni auttaa muita löytämään tämän teknologian olemassaolon ja innostaa perehtymään siihen tarkemmin, sillä massakäytöstään huolimatta se tuntuu edelleenkin olevan melko tuntematon käsite hyvin monelle ohjelmisto- sekä pelinkehittäjälle. Itse sain kuulla tästä teknologiasta sattumalta eräässä pelikonferenssissa, ja vasta sen jälkeen olen alkanut näkemään sitä kirjaimellisesti kaikkialla. Haluan tällä työlläni päivittäväni teknologian näkyvyyttä ja motivoivani muita inspiroitumaan NFC-teknologian hyödyntämiseen.

## Lähteet

Absolute Astronomy. 2017. Bluetooth.

<http://www.absoluteastronomy.com/topics/Bluetooth#encyclopedia>.  
3.3.2017.

Android Developers. 2017a. NFC Basics.

<https://developer.android.com/guide/topics/connectivity/nfc/nfc.html>.  
12.3.2017.

Android Developers. 2017b. Android.nfc

<https://developer.android.com/reference/android/nfc/package-summary.html>. 12.3.2017.

Codexpedia. 2017. Android NFC Read and Write example.

<http://www.codexpedia.com/android/android-nfc-read-and-write-example/>. 12.3.2017.

Framentos Developers. 2013. How to write "Hello World" into a NFC tag in Android.

<http://www.framentos.com/en/android-tutorial/2012/07/31/write-hello-world-into-a-nfc-tag-with-a/>. 12.3.2017.

Jyväskylän Yliopisto. 2014. Tutkimusstrategiat.

<https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/>. 3.3.2017.

NFC Forum, 2015. NFC Forum Brings Advanced Security to NFC Tags with Signature RTD 2.0 Technical Specification.

<http://nfc-forum.org/newsroom/nfc-forum-brings-advanced-security-to-nfc-tags-with-signature-rtd-2-0-technical-specification-2/>.  
22.12.2016.

RFID Lab Finland Ry, 2017a. Mitä on RFID.

<http://www.rfidlab.fi/rfid-teknologia/mita-on-rfid/>. 10.05.2017.

RFID Lab Finland Ry, 2017b. NFC.

<http://www.rfidlab.fi/rfid-teknologia/nfc/>. 10.05.2017.

RFID Lab Finland Ry, 2017c. RFID-teknologian soveltamisalueita.

<http://www.rfidlab.fi/rfid-teknologia/soveltamisalueet/>. 10.05.2017.

Salmi, T. 2007. Radiotaajuinen etätunnistus.

<http://publications.theseus.fi/bitstream/handle/10024/11934/2008-03-19-08.pdf?sequence=1>. 21.12.2016.

Sunsero, 2017. RFID-tunnisteet.

[http://www.sunsero.fi/rfid\\_tunnisteet/](http://www.sunsero.fi/rfid_tunnisteet/). 10.05.2017.

Tap into NFC. 2016. Knowledge base: Android.

<http://tapintonfc.org/knowledgebase/android/>. 21.12.2016.

Tech Radar. 2015. What is NFC? Everything you need to know.

<http://www.techradar.com/news/phone-and-communications/what-is-nfc-and-why-is-it-in-your-phone-948410/3>. 21.12.2016.

Thrasher, J. 2013. RFID vs NFC: What's the difference?

<http://blog.atlasrfidstore.com/rfid-vs-nfc>. 10.05.2017.

What is a QR Code?. 2017.

<http://www.whatisaqrcoode.co.uk/>. 20.4.2017.

Wikipedia. 2016. RFID.

<https://fi.wikipedia.org/wiki/RFID>. 21.12.2016.

Wikipedia. 2017a. Near Field Communication.

[https://en.wikipedia.org/wiki/Near\\_field\\_communication](https://en.wikipedia.org/wiki/Near_field_communication). 21.12.2016.

Wikipedia. 2017b. List of gaming NFC platforms.

[https://en.wikipedia.org/wiki/List\\_of\\_gaming\\_NFC\\_platforms](https://en.wikipedia.org/wiki/List_of_gaming_NFC_platforms).  
21.12.2016.

Wondratschek, R. 2013a. Reading NFC Tags with Android.

<https://code.tutsplus.com/tutorials/reading-nfc-tags-with-android--mobile-17278>. 3.3.2017.

Wondratschek, R. 2013b. Reading NFC Tags with Android.

[https://cdn.tutsplus.com/mobile/uploads/2013/05/Reading-NFC-Tags-with-Android\\_3.png](https://cdn.tutsplus.com/mobile/uploads/2013/05/Reading-NFC-Tags-with-Android_3.png). 3.3.2017.