POHJOIS-KARJALAN AMMATTIKORKEAKOULU
Tietojenkäsittelyn koulutusohjelma

Anne-Mari Valtonen

MOBIILIN LÄHIMAKSAMISEN MAHDOLLISUUDET

Opinnäytetyö
Kesäkuu 2012

POHJOIS-KARJALAN
AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Kesäkuu 2012
Tietojenkäsittelyn koulutusohjelma

Länsikatu 15
80110 JOENSUU

Tekijä
Anne-Mari Valtonen

Nimeke
Mobiilin lähimaksamisen mahdollisuudet

Toimeksiantajat
TG4NP-hanke ja Digiregion-hanke

Tiivistelmä

Opinnäytetyössä perehdytään mobiilimaksamiseen ja varsinkin mobiilin lähimaksamisen tilanteeseen vuonna 2012 ja tulevaisuudessa. Tavoitteena oli saada aikaan kattava katsaus, jossa käsitellään tämänhetkistä tietoa mobiilimaksamisen vaihtoehdoista ja NFC-teknologian sovellutusmahdollisuuksista. Selvitykselle on ollut tarvetta lähimaksamisen ja NFC-teknologian käytön yleistymisen myötä.

Opinnäytetyössä käsitellään aluksi yleistietoa mobiilimaksamisesta, kerrotaan kuinka erilaisia maksuratkaisuja on jaoteltu ja mitä erilaisia vaihtoehtoja etä- ja lähimaksamiseen on tällä hetkellä olemassa. Työssä keskitytään selvittämään erityisesti lähimaksamisessa käytettävää NFC-teknologiaa. Maksamisen lisäksi NFC:tä voidaan hyödyntää myös lukuisissa muissa sovellutuskohteissa. NFC:stä käsitellään sen toimintaperiaatetta, maksamisen nykytilannetta sekä tulevaisuuden näkymiä. Työhön on kerätty esimerkkejä teknologian sovellutuksista erilaisissa käyttökohteissa, selvitetty käytön turvallisuutta sekä teknologian kehityksessä ilmenneitä haasteita. NFC-teknologian hyödyntämisen havaittiin olevan tällä hetkellä vielä melko alkuvaiheessa eikä kehitystyö ole vielä kaikilta osin täysin valmis.

Opinnäytetyön tiedot kerättiin laajasti internetin eri lähteitä käyttäen. Työn tuloksena syntyi raportti, jonka avulla saadaan jaettua tietoa toimeksiantajien ja kaikkien aiheesta kiinnostuneiden käyttöön.

Kieli
suomi

Sivuja 85

Asiasanat
Mobiilimaksaminen, lähimaksaminen, NFC

NORTH KARELIA
UNIVERSITY OF APPLIED SCIENCES

THESIS
June 2012
Degree Programme in Business Information Technology
Länsikatu 15
80110 JOENSUU
FINLAND

Author
Anne-Mari Valtonen

Title
Possibilities of Mobile Local Payment

Commissioned by
TG4NP-project and Digiregion-project

Abstract

At first this thesis focuses on mobile payments and especially the situation in 2012 and in the future. The aim was to provide a comprehensive review which deals with the current information about the mobile payment options, and technology applications in the NFC. The study was needed because local payment and the use of NFC technology have become more prevalent.

First some general information about mobile payments is introduced. The study explains how a variety of payment solutions are classified and what the different options for remote, proximity and local payments are currently available. The focus will be to examine the NFC technology used in local payment in particular. In addition to the payments the NFC can also be used to many other applications. The thesis will deal with the NFC operation principles, the current situation of payments as well as future prospects. Examples of technology applications in a variety of applications were collected, the safety of use was explained, and finally, the challenges encountered in the evolution of technology. Utilising NFC technology was found to be still in relatively early stages at present and the development of technology is yet not complete.

Information for the thesis was collected widely from different sources of the Internet. The result was a report, which provides the commissioner with shared data and all who are interested in this topic.

Language
Finnish

Pages 85

Keywords
Mobile payment, local payment, NFC

Sisältö

Lyhenteet

Aktiivitunniste	Omalla virtalähteellä varustettu RFID-tunniste. Aktiivitunnisteiden avulla on mahdollista saavuttaa hyvin pitkät lukuetäisyydet. (RFID Lab Finland ry 2012a.)
Antenni	Tiedon välittämiseen käytettävä osa, joka sijaitsee lukijassa tai tunnisteessa (RFID Lab Finland ry 2012a).
Appletti	Web-selainympäristössä toimiva lyhyt Java-ohjelma. Applettien avulla voidaan lisätä verkkosivuille esimerkiksi dynaamista tekstiä tai animaatioita. (Urbaani Sanakirja 2012.)
Autentikointi	Todennus, eli palvelun tai käyttäjän identiteetin varmistaminen (Jyväskylän yliopisto 2012).
Bluetooth	Teknologia, jota käytetään heikkotehoisella radioyhteydellä luomaan linkkejä puhelimien, tietokoneiden ja muiden verkkolaitteiden välille (Mitchell 2012).
CPU	Central Processing Unit. Esimerkiksi matkapuhelimessa oleva suoritin, joka suorittaa ohjelman konekielisiä käskyjä. (Wikipedia 2012a.)
Emulointi	Emuloinnissa järjestelmä imitoi tai kopio toista järjestelmää. Tämä voidaan tehdä käyttämällä laitteistoa, ohjelmistoa tai näiden yhdistelmää. (TechTerms 2008.)
EMV	Europayn, Mastercardin ja Visan kehittämä maksujärjestelmien sirukorttistandardi (NFC-työryhmä 2010, 5).
ERC	Euroopan radioviestintäkomitea. Nykyisin ECC, eli Euroopan sähköisen viestinnän komitea. (Viestintävirasto 2004.)
ETSI	European Telecommunications Standards Institute. Eurooppalainen telealan standardisoimisjärjestö. (SFS ry 2012.)
Etämaksaminen	Maksu välitetään maksun saajalle tietoliikenneverkon kautta (Tuominen 2003, 2). Maksajan fyysisellä sijainnilla ei ole merkitystä maksuhetkellä (Kapanen 2010, 4).
HF	High-Frequency. Taajuusalue, joka on käytännössä 13,56 MHz. (RFID Lab Finland ry 2012a.)
Jammeri	Radiolähetin, jota käytetään radioliikenteen häirintään.

Kryptografia	Salaaminen/salakirjoitus. Käytetään yleisimmin suojaamaan internet-liikennettä. (Wikipedia 2012b.)
LF	Low-Frequency. Taajuusalue, joka on käytännössä 125 kHz tai 134 kHz. (RFID Lab Finland ry 2012a.)
Lähimaksaminen	Maksutapahtuma, jossa ostajan päätelaitteen ja myyjän maksupäätteen välillä ei tarvita ollenkaan ulkoista tietoliikenneverkkoa, eli maksu voi siirtyä suoraan maksajan päätelaitteesta myyjän maksupäätteelle (local payment). Lisäksi voidaan tarkoittaa lähimaksuympäristöä, missä fyysinen etäisyys maksajan ja maksun vastaanottajan välillä on pieni (proximity payment). (Tuominen 2003, 2 - 3.)
Makromaksu	Käytetään mikromaksuja suurempien ostosten maksamiseen (noin 10 eurosta ylöspäin), joten myös turvallisuusvaatimukset ovat tiukempia (Tuominen 2002, 9 - 10).
M-commerce	Mobile commerce. Tuotteiden ja palveluiden ostaminen ja myyminen onnistuu mobiililaitteen avulla. (Rouse 2005.)
Mikroaalto	Yleisin taajuus mikroaaltoalueella on 2,4 GHz. Mikroaaltoja käytetään suurimmaksi osaksi aktiivitunnistuksessa, jossa tunnisteen sisällä on oma virtalähde. (RFID Lab Finland ry 2012b.)
Mikromaksu	Pieni rahallinen maksu hyödykkeestä. Yleisesti käytössä, kun halutaan kuluttajan maksavan tuotteesta tai palvelusta pieni korvaus. (Uimonen 2003.)
Mobiililaite	Laite, jolla pääsee tietoverkkoon ajasta tai paikasta riippumatta. Esimerkiksi älypuhelimet, kannettavat tietokoneet, tabletit sekä laitteet, joiden ominaisuudet hävittävät laitteiden väliset rajat. (Mobiiliopas 2012.)
Mobiilimaksaminen	Matkapuhelimen tai muun mobiililaitteen avulla suoritettava kahden eri osapuolen välinen rahanvaihto. Tapahtumassa saadaan vastapalveluksi joko tuotteita tai palveluita. (Mobile Payment Forum 2002, 10.)
Mobile tagging	Mobiili koodaus, jossa luetaan kaksiulotteisia tunnisteita käyttämällä lukulaitteena matkapuhelinta. Tunnisteet voivat esimerkiksi ohjata käyttäjän jollekin internetsivustolle. (NFC-työryhmä 2010, 5.)
Modulointi	Modulointimenetelmillä lähetetään tietoa siirtotien (esimerkiksi radioaaltojen) välityksellä. Siirrettävä tieto sovitetaan siirtotielle moduloimalla. (Wikipedia 2012c.)

NDEF-formaatti	NFC Data Exchange Format. Käytetään määrittelemään viestin kapselointia viestin välityksessä kahden NFC-laitteen tai NFC-laitteen ja tunnisteen välillä. (Radio-Electronics.com 2012.)
NFC	Near Field Communication. Lyhyen etäisyyden kontaktiton yhteysteknologia, joka yhdistää laitteiden välisen tunnistamisen ja kommunikoinnin langattomasti. (Sunsero 2012.) Perustuu RFID-tekniikkaan.
OTA	Over The Air. Standardi sovelluksiin liittyvien tietojen lähettämisen ja vastaanottamiseen langattomassa kommunikointisysteemissä. (Rouse 2007.)
Passiivitunniste	Tunniste saa käyttövirtansa RFID-lukijasta ilmateitse. Suunniteltu usein kertakäyttöisiksi. (RFID Lab Finland ry 2012a.)
PayPal	Erittäin suosittu maksutapa, kun tehdään ostoksia internetissä. PayPal tarjoaa kansainvälisen maksujenvälityspalvelun, jonka kautta voidaan siirtää rahaa ympäri maailman ja maksaa ostoksia (PayPal 2012a).
PDA	Personal Digital Assistant, eli kämmentietokone (Wikipedia 2012d).
P2P	Voi tarkoittaa käsitettä person to person tai peer to peer. Kahden henkilön tai laitteen välinen tiedonsiirto.
RFID	Radio Frequency IDentification. Tekniikka, joka mahdollistaa radiotaajuuksilla tapahtuvan tunnistamisen. Käytetään tunnisteiden sisältämän tiedon tallentamiseen ja langattomaan lukemiseen RFID-lukijalla. (RFID Lab Finland ry 2012c.)
RFID-lukija	Mahdollistaa RFID-tunnisteen lukemisen ja kirjoittamisen. Sisältää antennin ja lukulaitteen. Liitetään yleensä tietokoneeseen tai kenttäväylään. Lukijalaite voi olla pienempi levymuotoinen antenni, portti tai kannettava käsipääte. (RFID Lab Finland ry 2012a.)
RFID-tunniste	RFID-tunniste sisältää tietoa, jota voi tunnisteesta riippuen lukea ja kirjoittaa. Voi olla muodoltaan esimerkiksi kortti, tarra, nappi tai vastaava. Sisältää antennin ja sirun. Muita kutsumanimiä ovat esimerkiksi "älytarra", "saattomuisti", "RFID-tägi" sekä ”inletti”. (RFID Lab Finland ry 2012a.)
SATSA	Security and Trust Services API. Laajennus, jota voidaan käyttää mobiilimaksamisessa tai muissa erikoisti-

	lanteissa, joissa käytetään SIM-korttia. (Kainulainen 2011.)
SE	Secure Element. Älysiru, jota kutsutaan turvaelementiksi. Mahdollistaa matkapuhelimen tallentaa turvallisesti maksuohjelman, sekä käyttäjän tilitiedot, ja käyttää näitä tietoja toimiessaan kuten maksukortti. (Smart Card Alliance 2012.)
SWP-protokolla	Single Wire Protocol. Mahdollistaa mobiilimaksamisen operaatorin tarjoamalla NFC-SIM-kortilla. (Kolehmainen 2011a.)
UHF	Ultra High Frequency. Korkean taajuuden RFID-tekniikka. RFID-sovelluksissa 865 - 928 MHz. Tunnisteiden lukuetäisyys on pidempi kuin 13,56 MHz tunnisteiden ja myös lukunopeus on korkeampi. Toisin kuin 13,56 MHz:n teknologiassa, antenni ei indusoi (aikaansaa) virtaa tunnisteeseen kuten muuntaja, vaan tunnisteen tunnistaminen perustuu radioaaltoihin ja niiden takaisin heijastumiseen tunnisteen dipoliantennista. (RFID Lab Finland ry 2012a.)
UICC	Universal Integrated Circuit Card. Älykortti, joka sisältää GSM-verkon SIM-sovelluksen, sekä mahdollisesti 3G-verkon USIM-sovelluksen. Kortti voi sisältää myös muita sovelluksia, kuten maksusovelluksen tai matkakorttisovelluksia. Kortti voi sisältää myös SWP-tuen puhelimen NFC-sirulle. (FiCom ry 2008, 4 - 5.)
UWB-tiedonsiirto	Ultra wideband. UWB-tekniikka mahdollistaa nopean sisätilan tiedonsiirtoyhteyden. Tiedon siirtäminen tapahtuu pienellä tehotasolla lyhyiden kantataajuisten pulssien avulla. (Hämäläinen 2002.)
WAP	Tulee sanoista Wireless Application Protocol. Langattomien sovellusten protokolla, joka mahdollistaa internetin tai intranetin hyödyntämiseen mobiililaitteessa. (Karinen 2004.)
WLAN	Wireless Local Area Network. Tätä langatonta lähiverkkotekniikkaa käytetään yhdistämään langattomasti erilaiset verkkolaitteet. (Wikipedia 2012e.)

1 Johdanto

Mobiilimaksaminen on aiheena laaja ja monille myös varsin tuntematon. Suuri osa ihmisistä kuljettaa päivittäin mukanaan matkapuhelinta tai muuta mobiililaitetta, jota pystytään nykyaikana hyödyntämään yhä monipuolisemmissa sovellutuskohteissa. Matkapuhelimesta on tullut monille niin tärkeä, että ilman sitä ei enää haluta lähteä ulos. Jopa lompakko jätetään kotiin mieluummin. (Leidenius 2007.) Pienten ostosten etämaksaminen tekstiviestillä tai puhelinsoitolla on tuttua monille, mutta kehitys on tehnyt mahdolliseksi myös esimerkiksi kaupasta ostettavien päivittäisten hankintojen lähimaksamisen nopeasti ja helposti vain käyttämällä NFC-sirun sisältävää matkapuhelinta, tarraa tai älykorttia maksupäätteen luona. NFC-tekniikkaa hyödyntävä lähimaksaminen onkin oivallinen vaihtoehto korvaamaan vaivalloisempia maksutapoja, kuten käteisellä maksamista tulevien vuosien aikana. (Luottokunta 2011a, 1 - 2.) Maksamisen lisäksi matkapuhelin voi toimia myös esimerkiksi avaimena, lippuna tai henkilöllisyystodistuksena. Hyödyntämismahdollisuudet ovat erittäin laajat.

Raportissa tarkastellaan mobiilimaksamisen tilannetta keskittyen erityisesti lähimaksamisen ja NFC-tekniikan tämänhetkisiin mahdollisuuksiin ja tulevaisuuden näkymiin. Lähitunnistuksen laajempi käyttöönotto on ollut hidasta teknisten ongelmien ja standardien puuttumisen lisäksi myös kuluttajien yksityisyydensuojaan liittyvien epävarmuustekijöiden vuoksi (NFC-työryhmä 2010, 13 - 15).

Työssä käydään läpi ensimmäisenä yleistä tietoa mobiilimaksamisesta, minkä jälkeen selvitetään miten erilaisia maksuratkaisuja on jaoteltu ja mitä erilaisia vaihtoehtoja etä- ja lähimaksamiseen on tällä hetkellä olemassa. Työssä otetaan selvää muun muassa etä- ja lähimaksamisen vaihtoehtojen käyttäjäystävällisyydestä, käytön yleisyydestä, ongelmista sekä tekniikan rajoituksista. Maksamisen lisäksi NFC:tä voidaan hyödyntää myös lukuisissa muissa sovellutuskohteissa, joita tarkastellaan työssä maksamisen ohella. Opinnäytetyön toimeksiantajina on kaksi hanketta. Tarkoituksena on saada raportin avulla tämän hetkistä tietoa toimeksiantajien sekä kaikkien mobiilimaksamisen ja NFC:n mahdollisuuksista kiinnostuneiden käyttöön.

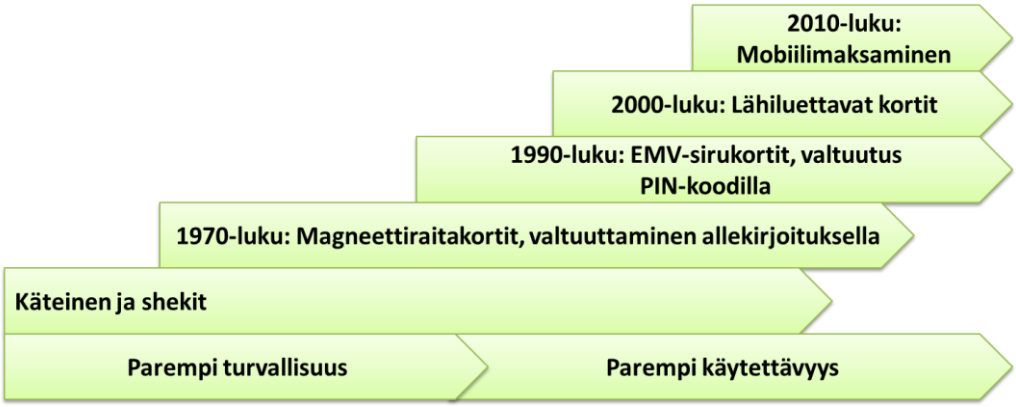
2 Yleistä mobiilimaksamisesta

Mobile Payment Forum määrittelee mobiilimaksamisen kahden eri osapuolen väliseksi rahanvaihdoksi, joka suoritetaan mobiililaitteen avulla. Tapahtumassa saadaan vastapalveluksi joko tuotteita tai palveluita. Mobiililaitteeksi voidaan lukea langatonta yhteyttä käyttävä laite, kuten matkapuhelin, PDA (kämmentietokone), tabletti tai kannettava tietokone. (Mobile Payment Forum 2002, 10.) Suomessa mobiilimaksamista säätelee luottolaitoslaki, joka määrittelee mitä luottolaitostoiminnassa kukakin saa tarjota (Tuominen 2003, 19 - 23). Maksutapa on ollut jollakin tavalla käytössä jo yli kymmenen vuoden ajan. Sonera esitteli vuonna 1997 ostosautomaattiratkaisunsa, jossa asiakkaan oli mahdollista ostaa tuote soittamalla puhelimella annettuun numeroon. Ostokset laskutettiin asiakkaan puhelinlaskun yhteydessä. Sittemmin tekstiviestimaksaminen on yleistynyt hyvin käyttöliittymäksi sisältöpalveluihin ja tullut vaihtoehdoksi puhelinsoitolla tapahtuvan maksamisen rinnalle. (Tuominen 2003, 1.) Sisältöpalveluiden markkinat ovat kasvaneet koko palveluiden tarjonnan historian ajan, kun oman matkapuhelimen sisältöä on haluttu mukauttaa entistä enemmän omanlaiseksi erilaisten immateriaalituotteiden, kuten taustakuvien, soittoäänien ja pelien avulla. (Prisma Research Oy 2006, 44 - 46.)

Myös prepaid-tilin avaaminen oli varsinkin 2000-luvun alkupuolella suosiossa. Tässä maksutavassa käyttäjä tallettaa prepaid-tililleen rahaa, minkä jälkeen maksuja on mahdollista hoitaa tililtä tekstiviestein. Vuonna 2002 ryhdyttiin yhdistämään tekstiviestimaksamista Luottokunnan luottokorttitileihin. Tuolloin myös lanseerattiin mobiilimaksukukkaron yhdistelmät, jotka sijoitettiin tekstiviestin ja verkkopankin yhteyteen. Suomessa pankkien mobiileista rahakukkaroratkaisuista suosituimmiksi päätyivät jo sittemmin lopetetut Sampo Pankin, Nordean ja Radiolinjan Mobiiliraha sekä Osuuspankin Digiraha. (Tuominen 2003, 1 - 10.)

Mobiilimaksamisen viimeaikainen merkittävä kehitys antaa aiheen kysyä, olemmeko jo mobiilin maksamisen nopean yleistymisen kynnyksellä, vai jatkuuko kehitys jatkossakin tasaisen hitaalla tahdilla. Mobiilimaksamisen viimeaikais-

ta kehitystä on vauhdittanut mobiililaitteiden, kuten älypuhelinten nopea yleistyminen yhä useamman käyttöön. Käyttäjät myös kiintyvät yhä enemmän mobiililaitteisiinsa niiden tarjotessa yhä monipuolisemman käyttökokemuksen arjen helpottamisessa ja näin myös mobiilimaksaminen kiinnostaa yhä suurempaa määrää kuluttajista. (Innopay 2011, 9.) Mobiilimaksamisessa on nähtävissä läpimurto massamarkkinoille lähivuosien aikana (kuva 1).



Kuva 1. Maksamisen teknologinen kehitys (Kapanen 2010, 7).

2000-luvulla yleisin mobiilimaksutapa on ollut tilata hyödykkeitä tekstiviestillä tai puhelinsoitolla ja laskuttaa palvelut puhelinlaskulle (Tuominen 2003, 35). Varsinkin tekstiviestillä maksaminen on yhä tänä päivänä yleinen ja myös kaikkein laajimmin käytetty ratkaisu mobiilimaksamisessa (Innopay 2011, 16).

Mobiilimaksaminen kasvattaa suosiotaan teknologian kehittyessä. Taulukossa 1 havainnollistetaan tilastokeskuksen keräämien tietojen pohjalta matkapuhelinten käyttöä maksamiseen Suomessa vuonna 2011 (%-osuus väestöstä). Jaottelu on tehty henkilön iän, toiminnan, koulutuksen, asuinpaikan ja sukupuolen mukaan. Tilaston mukaan mobiilimaksamista hyödyntävät tällä hetkellä eniten nuoret aikuiset, opiskelijat sekä henkilöt, joilla on korkea-asteen koulutus. Eniten matkapuhelinta käytetään maksamisessa pääkaupunkiseudulla. Miehet käyttävät matkapuhelinta maksamisessa vain hieman naisia enemmän.

Taulukko 1. Matkapuhelimen käyttö maksamiseen Suomessa vuonna 2011 (Tilastokeskus 2011).

	Käyttänyt rahan asemasta matkapuhelinta maksamiseen 3 kk aikana	**Käyttää rahan asemasta matkapuhelinta maksamiseen viikoittain**
	%-osuus väestöstä	
16 - 24 v	11	1
25 - 34 v	16	3
35 - 44 v	13	1
45 - 54 v	7	1
55 - 64 v	4	0
65 - 74 v	3	0
Opiskelijat	12	1
Työlliset	10	1
Eläkeläiset	3	0
Perusasteen koulutus	7	1
Keskiasteen koulutus	7	1
Korkea-asteen koulutus	12	1
Pääkaupunkiseutu	17	3
Suuret kaupungit	10	1
Muut kaupunkimaiset kunnat	7	1
Taajaan as/maaseutum. kunnat	5	0
Miehet	10	2
Naiset	7	0
Yhteensä	9	1

Tällä hetkellä merkittäväksi lähimaksutavaksi on nousemassa NFC-teknologiaan perustuva lähimaksaminen joko matkapuhelimen, älykortin tai tarran avulla. Luottokunnan (2012a) mukaan kontaktittoman maksamisen odotetaan korvaavan muita vaivalloisempia maksutapoja, kuten käteisellä rahalla maksamista lähitulevaisuudessa ainakin pienempien maksujen osalta.

2.1 Mobiilimaksuratkaisujen jaottelu

Erilaisia mobiilimaksuratkaisuja jaotellaan karkeasti erilaisiin maksutyyppeihin maksuetäisyyden, maksun suuruuden sekä veloitustavan mukaan.

2.1.1 Maksuetäisyys

Mobiilimaksut jaotellaan maksuetäisyyden, eli toisin sanoen sen mukaan, kuinka kaukana maksutapahtuman eri osapuolet sijaitsevat maksuhetkellä toisistaan. Etäisyysjaottelussa mobiilimaksut jaetaan etä- ja lähimaksuihin.

Etämaksut

Etämaksamisella tarkoitetaan maksutapahtumaa, jossa maksajan tai myyjän fyysisellä sijainnilla ei ole merkitystä. Maksaminen voidaan suorittaa tekstiviesteillä (tai soittamalla), sekä käyttämällä matkapuhelimen selainominaisuuksia tai älypuhelinten maksusovelluksia. (Kapanen 2010, 4.) Maksu välitetään maksun saajalle matkaviestinverkon kautta (Tuominen 2003, 2 - 4). Tästä maksutavasta on lisätietoa luvussa 2.2.

Lähimaksut

Lähimaksamisella voidaan tarkoittaa maksutapahtumaa, jossa maksu välitetään maksajan mobiililaitteelta suoraan myyjän maksupäätteelle ilman ulkoista tietoliikenneverkkoa (”local payment”). Lisäksi voidaan tarkoittaa lähimaksuympäristöä, jossa maksajan ja maksun vastaanottajan fyysinen etäisyys on lyhyt, eikä siirtomedialla ole merkitystä (”proximity payment”). (Tuominen 2003, 2.)

2.1.2 Maksun suuruus

Mobiilimaksut jakautuvat maksun suuruuden mukaan mikro- ja makromaksuihin. Jaotteluun vaikuttaa maksun suuruus, sekä maksutavalta vaadittu tunnistautumistapa ja tietoturvallisuuden taso.

Mikromaksut

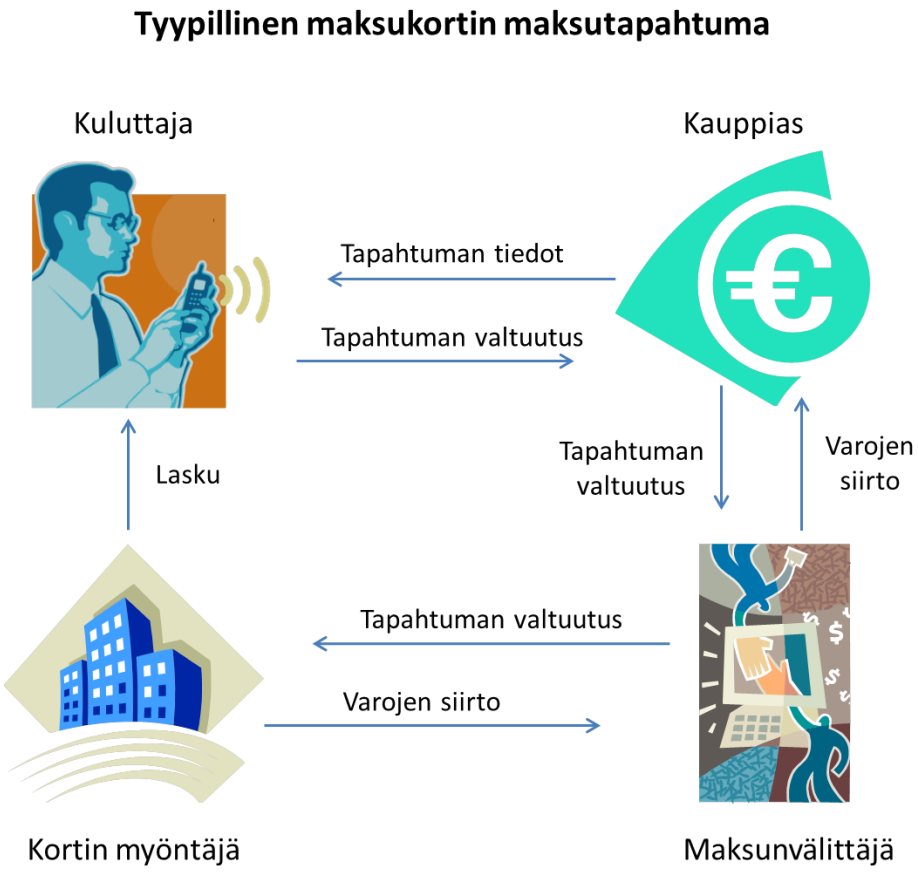
Mikromaksuja käytetään pienten ostosten maksamiseen. Tällaisia ostoksia voivat olla esimerkiksi verkkopelit, uutispalvelut tai musiikki. Yksittäinen mikromaksu voi olla alimmillaan jopa alle sentin suuruinen. (Sanastokeskus TSK 2007.) Suurin sallittu maksun suuruus vaihtelee maksunvälittäjien mukaan tällä hetkellä noin 10 ja 25 euron välillä. Esimerkiksi PayPal hyväksyy mikromaksuiksi noin 12 dollarin (eli noin 10 euron) suuruiset maksut (PayPal 2012b). Visa taasen hyväksyy alle 20 euron suuruiset maksut (Luottokunta 2012a). Mikromaksamisella tehtävät ostokset ovat hinnaltaan edullisia, minkä vuoksi tunnusluvulla tapahtuvaan kuluttajan henkilöllisyyden tunnistamiseen ei ole niin suurta tarvetta, kuin tehtäessä suurempia ostoksia (Luottokunta 2012b).

Makromaksut

Makromaksuja käytetään suurempien, noin 10 eurosta ylöspäin maksavien ostosten maksamiseen. Mikromaksuista poiketen tämän maksutavan käyttäminen vaatii erittäin vahvan panostuksen turvallisuuteen. (Tuominen 2002, 9 - 10.)

2.1.3 Veloitustavat

Maksutapahtuman perusperiaate ei muutu järjestelmästä tai teknologiasta huolimatta. Maksutilanteessa asiakas ottaa yhteyttä mobiililaitteellaan palveluun ja lähettää tapahtuman valtuutustiedon palveluntarjoajalle (kuva 2). Ostajan henkilöllisyys ja maksukyky tarkistetaan, minkä jälkeen lähetetään kuittaus ostotapahtuman onnistumisesta. (Mobile Payment Forum 2002, 7 - 8.)



Kuva 2. Tyypillinen maksukortin maksutapahtuma (Mobile Payment Forum 2002, 8).

Maksamisen voi hoitaa reaaliaikaisen maksamisen lisäksi jo etukäteen käyttämällä esimerkiksi prepaid-korttia. Lisäksi maksun voi suorittaa myös jälkikäteen esimerkiksi luottokortilla, puhelinlaskulla tai muulla erillisellä laskulla. (Fujitsu 2009.)

Puhelinlasku

Ostokset on mahdollista maksaa soittamalla tai lähettämällä tekstiviesti maksulliseen numeroon, jolloin hyödyke maksetaan puhelinlaskussa (Siru Mobile Oy 2012a). Maksutapa on saatavilla helposti, koska maksamiseen ei tarvita erillistä lisäohjelmaa. Maksutapahtumassa ei liiku maksajasta puhelinnumeroa lukuun ottamatta mitään muita henkilökohtaisia tietoja, joten maksutapa on turvallisempi verrattuna pankki- ja luottokorttien käyttöön. (Siru Mobile Oy 2012b.)

Käytön turvallisuutta lisää kuluttajansuoja, jonka periaatteen mukaan kuluttajalla on oikeus saada maksutta varmistus laskun oikeellisuudesta tekstiviestien ja puheluiden lisäksi myös maksutapahtumien osalta. Maksupalvelulaki säätelee tiedot, jotka palveluntarjoajan on annettava erillisistä maksutapahtumista. (Kuluttajavirasto 2009.)

Puhelinlaskulla maksettaessa voi ilmetä ongelmia verottajan kanssa varsinkin, mikäli maksamiseen käytetään työsuhdepuhelinta. Puhelinlaskussa maksettavat ostokset tuottavat ongelmia lisäksi myös operaattoreille, koska niissä piilee luottoriski. (Fujitsu 2009.)

Rahakukkaro

Tässä maksutavassa asiakas siirtää erikseen rahaa verkkopankin prepaid-tilille, jonka varoja hallitaan matkapuhelimella palvelunumeroon lähetettävien tekstiviestien avulla. Tämä maksutapa esiteltiin vuonna 2002, kun Osuuspankki lanseerasi Digiraha-palvelun. Myös Nordea ja Sampo kehittivät yhteistyössä Radiolinjan kanssa oman Mobiilirahakonseptinsa, joka julkistettiin samana vuonna. (Tuominen 2003, 10 - 13.) Palveluissa saman tilin sisäisissä siirroissa ei tarvittu tilisiirtoa, joten kustannukset olivat moniin muihin verkkomaksuvälineisiin verrattuna pienemmät. Palvelu ei kuitenkaan koskaan päässyt kunnolla käyntiin kuluttajien vähäisen kiinnostuksen vuoksi. Lisäksi vuonna 2010 käytäntöön tullut maksupalvelulaki asetti ostoksille ylärajaksi 30 euroa, mikä rajoitti palvelua entistä epäkäytännöllisemmäksi. Lopulta Digiraha-palvelu lopetettiin vuonna 2011. (Frilander 2011.) Mobiiliraha-palvelu oli käytössä Suomessa vuosina 2004 - 2007 (Koskinen 2011).

Digirahan ja Mobiilirahan jälkeen samantapainen järjestelmä on edelleen yhdysvaltalaisella kansainvälisesti toimivalla PayPal-maksujenvälitysjärjestelmällä, sekä useilla muilla vastaavanlaisilla järjestelmillä. Myös PayPalin järjestelmässä rahaa ladataan erilliselle PayPal-tilille, tai tili on kytketty pankkitiliin tai luottokorttiin, josta sitä voi vapaasti siirtää verkossa esimerkiksi siirrettäessä rahaa toisille kukkaron omistajille tai maksettaessa ostoksia. PayPal on keskittynyt suurimmaksi osaksi internetissä tapahtuvaan maksunvälitykseen. (PayPal 2012a.)

Yritys on kuitenkin kiinnostunut mobiilimaksamisen mahdollisuuksista ja on testannut lähimaksamista jo muun muassa Ruotsissa (Kolehmainen 2011b).

Luottokortti

Esimerkiksi Luottokunnan tarjoamalla kontaktittomalla maksamisella ostaja voi suorittaa alle 20 euron suuruiset maksut alle sekunnissa joko matkapuhelimella tai kortilla. Tekniikkaa käytetään jo tällä hetkellä eri puolilla Eurooppaa pienten maksujen suorittamiseen. (Luottokunta 2012a.) NFC-teknologiaa hyödyntävällä kortilla maksettaessa esimerkiksi Visa PayWaven avulla, voidaan maksu suorittaa nopeasti vain käyttämällä korttia lukijalaitteen lähellä. Tällöin ei ole tarvetta antaa edes tunnuslukua. Ratkaisu mahdollistaa korttien paremman käytettävyyden tapahtumissa, joissa käteinen on yleisin maksuväline. Käyttökohteita ovat esimerkiksi pikaruokaravintolat, julkinen liikenne ja erilaiset myyntiautomaatit. Näissä tilanteissa saadaan hyötyä myös lyhenevistä kassajonoista. Suuremmissa maksuissa käytetään edelleen kortilla olevaa sirua sekä kortin tunnuslukua. (Luottokunta 2012c.) Matkapuhelimella suoritettavassa kontaktittomassa maksamisessa NFC-ominaisuus voi olla puhelimessa itsessään tai siinä käytettävässä SIM-kortissa. Maksaminen tapahtuu kuten kortilla, mutta tällöin riittää, että puhelin viedään lukijalaitteen lähelle. Puhelimella yli 20 euron suuruisia maksuja suoritettaessa vaaditaan puhelimeen kirjattavaksi tunnusluku, ennen kuin puhelin viedään lukijalaitteen lähellä maksun suorittamiseksi. (Luottokunta 2012b.)

2.2 Etämaksaminen

Lähimaksamisesta poiketen etämaksutilanteessa maksajan fyysisellä sijainnilla ei ole merkitystä. Maksaminen voidaan suorittaa tekstiviesteillä (tai soittamalla), sekä käyttämällä matkapuhelimen selainominaisuuksia tai älypuhelimen maksusovelluksia. (Kapanen 2010, 4.) Suoritettava maksu välitetään tietoliikenneverkon (matkaviestinverkon) kautta (Tuominen 2003, 2 - 3.)

2.2.1 Maksaminen tekstiviestillä

Hyödykkeiden maksaminen SMS-maksupalvelun kautta on tällä hetkellä suosittu mobiilimaksamiseen käytettävä maksutapa nopeutensa ja helppoutensa ansiosta. Maksutapa soveltuu parhaiten pienten ostosten (0 - 20 euroa) maksamiseen. (Wired-Bit Oy 2012.) Ostoksia voivat olla esimerkiksi puhelimeen tilattavat soittoäänet, bussiliput, sähköisen lehden lukuaika tai autopesu (Movila 2012).

Esimerkiksi Wired-Bit Oy (2012), joka toimii internet- ja mobiiliratkaisujen toteuttajana, kertoo että tekstiviestimaksuissa teleoperaattorien kulut vähennetään maksusta kiinteällä 17 % osuudella, joka pienentää tulosta varsinkin suurten maksujen osalta. Maksullinen SMS-viesti on kuitenkin kustannustehokas pienissä maksuissa, kun sitä verrataan verkkopankkimaksuihin tai postituskuluihin. Taulukossa 2 on esimerkki tekstiviestien perushinnoittelusta.

Taulukko 2. Esimerkki SMS-viestien perushinnoittelusta (Wired-Bit Oy 2012).

Hinta / SMS (ALV 23 %)	Hinta / SMS (ALV 0 %)	Kk-maksu	Tuloutus	Wired-Bit Oy:n osuus	Operaattorien osuus
0,50 e	0,41 e	10 e /kk	66 %	17 %	17 %
1,00 e	0,81 e	10 e /kk	66 %	17 %	17 %
3,00 e	2,44 e	10 e /kk	66 %	17 %	17 %

Tyypillisessä maksutapahtumassa asiakkaalle annetaan ohjeet tekstiviestin lähettämiseen. Kun asiakas on lähettänyt viestin, hän saa paluuviestin mukana vahvistuskoodin ja kuittauksen maksusuorituksen onnistumisesta. Tekstiviestillä

maksettaessa veloitus lisätään automaattisesti asiakkaan puhelinlaskuun. (Siru Mobile Oy 2012c.)

Tekstiviestimaksamisen käyttömahdollisuudet ovat myös laajennettavissa, kun tekstiviestillä ostetaan suoran tuotteen sijasta kertakäyttöinen koodi, minkä kuluttaja voi vaihtaa reaalimaailman hyödykkeeseen. Tällaisia hyödykkeitä ovat esimerkiksi hampurilaisravintolan tuotteet tai teatterin sisäänpääsy. (Movila 2012.)

2.2.2 Maksaminen puhelinsoitolla

Maksaminen palvelunumeroon soittamalla on tekstiviestien ohella edelleen suosittu mobiilimaksamisen maksutapa pieniä ostoksia maksettaessa. Tässä maksutavassa asiakas soittaa maksulliseen numeroon ja seuraa saamiaan ohjeita. Puhelun päätyttyä asiakas voi esimerkiksi saada koodin, jolla pääsee käyttämään jotakin palvelua, kuten autopesua. (Alkio 2011.) Esimerkiksi VR:llä on käytössä mahdollisuus ostaa lippuja puhelinsoitolla. Lipun ostaja tarvitsee Credit/Debit-maksukortin, koska hänen tulee antaa korttinsa tiedot asiakasneuvojalle soittaessaan VR:n asiakaspalveluun. Liput toimitetaan joko matkapuhelimeen tai sähköpostiin. Yksi puhelu maksaa yhden euron. (VR-Yhtymä Oy 2011.) Soittamalla on mahdollista maksaa myös esimerkiksi pysäköintimaksuja, tilauksia joissakin pizzerioissa, autopesuja joillakin huoltoasemilla, sekä kalastuslupia metsähallitukselta. Yleensä laskutus tapahtuu suoraan puhelinlaskulle, mutta kuluttajille on suunniteltu myös palveluita, joihin rekisteröityessään asiakas voi halutessaan maksaa ostoksensa erillisellä laskulla. (Alkio 2011.)

Ongelmana puhelinsoitolla maksamisessa on ollut teleoperaattorien korkea provisio, joka voi nostaa hintaa huomattavastikin. Lisäksi myös tilityksessä on esiintynyt viivettä. (Tuominen 2003, 13.)

2.2.3 Maksaminen rahakukkarolla

Rahakukkaroa käytetään siirtämällä ensin rahaa verkkopankin virtuaaliselle tilille, minkä jälkeen ostoksia on mahdollista tilata operaattorin välitysjärjestelmästä. Tällöin välittäjä tunnistaa tilaajan henkilöllisyyden liittymän numeron perusteella ja veloittaa maksun pankissa olevasta mobiilirahakukkarosta. Kun henkilö on tunnistettu, ilmoittaa välittäjä tilauksen veloituksen onnistumisesta palvelun tarjoajalle ja asiakas saa ostamansa hyödykkeen. Pankki perii pankkitilin ja kukkaron välisestä rahansiirrosta tilisiirtoproviision. Asiakkaalta ei kuitenkaan peritä proviisiota kukkaron käytöstä. Pankin ja kauppiaan välinen rahansiirto tapahtuu palvelusopimuksen mukaisesti. Asiakas maksaa tekstiviestin lähettämisestä normaalin tekstiviestimaksun, joka peritään puhelinlaskussa. Tällaisia prepaid-tilejä ovat tuoneet kuluttajien saataville pankkien lisäksi myös useat muut palveluntarjoajat. (Tuominen 2003, 12 - 13.)

Rahakukkaron etuna on sen tietoturvallisuus. Asiakas pystyy tallettamaan erilliselle prepaid-tililleen kerralla vain tietyn summan rahaa (esimerkiksi enintään 250 euroa). Kukkaro on mahdollista lukita, mikäli käyttäjä kadottaa käyttäjätunnuksensa tai salasanansa, tai jos muuten on syytä epäillä, että kukkaron tiedot ovat joutuneet vääriin käsiin. (Digiraha 2008.)

Ongelmana prapaid-tilien käytössä on rahan tallettamisen vaivalloisuus. Rahaa on aina muistettava tallettaa tilille, jotta maksaminen sen kautta onnistuu. Maksuvälineen on kuitenkin toimittava heti ja ilman ylimääräisiä toimenpiteitä. Maksutapa on verrattavissa hyvin käteisellä maksamiseen. Kun asiakas nostaa rahaa pankkiautomaatista, hän usein maksaa ostoksensa kuitenkin mieluiten käteisellä, vaikka myös pankkikortti olisi mukana. Käteisellä maksamiseen verrattuna prepaid-tilin etuna on, että matkapuhelimeen voidaan ladata lisää käyttörahaa milloin ja missä vain. Kukkarotekniikka ei koskaan ole päässyt kuluttajien suosioon monista yrityksistä huolimatta, eikä tämän maksutavan enää odoteta nykyaikana yleistyvän. (Tuominen 2003, 8.)

2.3 Lähimaksaminen

Lähimaksamisella voidaan tarkoittaa kahta erillistä asiaa. Maksamisella voidaan tarkoittaa esimerkiksi kaupassa asioitaessa maksajan ja myyjän välistä lyhyttä fyysistä etäisyyttä (”proximity payment”), jolloin ei ole väliä sillä, mitä siirtomediaa maksamisessa käytetään. Vaihtoehtoisesti voidaan tarkoittaa myös maksamista, jossa ostajan päätelaitteen ja myyjän maksupäätteen välillä ei käytetä ollenkaan ulkoista tietoliikenneverkkoa, eli maksu siirtyy suoraan maksajan päätelaitteelta myyjän maksupäätteelle (”local payment”). Tällaisessa maksutapahtumassa käytetään lähikommunikointiin infrapunaa, Bluetoothia, tai RFID-piirejä (NFC). Tämän jaottelun lisäksi lähimaksaminen voidaan jakaa kahteen eri osaan myös sen mukaan, onko maksupaikalla asiakaspalvelijaa. Kun on kyse itsepalvelusta, puhutaan miehittämättömästä lähimaksamisesta (unattended point of sale). Asiakaspalvelijan ollessa paikalla, puhutaan miehitetystä lähimaksamisesta (attended point of sale). (Tuominen 2003, 2 - 3.)

Puhuttaessa mobiilista lähimaksamisesta, tapahtuu maksaminen hyödyntäen lähikommunikaatioteknologiaa. Mobiilissa lähimaksamisessa suoritettava maksu voidaan siirtää suoraan mobiililaitteesta kauppiaan maksupäätteelle ilman siihen erikseen tarvittavia maksunvälittäjiä. Toinen tapa on ensin tunnistaa maksaja, minkä jälkeen maksaminen tapahtuu taustajärjestelmien kautta. (Tuominen 2003, 2.)

Vielä tällä hetkellä ei ole laajalti käytössä mitään lähimaksutekniikoita, joten maksamisessa käytetään edelleen enimmäkseen etämaksutekniikkaa, kuten puhelinsoitolla tai tekstiviestillä suoritettavaa maksamista. Tällöin on kuitenkin kyse taustajärjestelmiä hyödyntävästä ”proximity paymentista”, eikä niinkään lähikommunikointiteknologiaa hyödyntävästä ”local paymentista”, josta kuitenkin ollaan tässä työssä eniten kiinnostuneita. (Tuominen 2003, 2.)

Kolmen eri siirtomedian sopivuutta lähimaksujärjestelmien pohjaksi on arvioitu Mobey Forumin tekemässä analyysissa seuraavasti:

Bluetooth

Bluetoothilla tarkoitetaan lyhyen kantaman radioteknologiaa, jonka kantaman pituus on noin 10 metriä. Se on kehitetty alun perin matkapuhelinten lisälaitteiden kytkentään. Bluetoothin merkittävin este mobiilimaksamiskäytössä on sen liian pitkä yhteydenmuodostamisaika, joka voi kestää 5 - 10 sekuntia. (Tuominen 2003, 16.)

Infrapuna

Infrapunalla suoritettavan tiedonsiirron toimintaetäisyys on noin metrin pituinen ja yhteyden muodostaminen onnistuu noin yhdessä sekunnissa. Infrapunan toiminta vaatii päätelaitteen ja maksupäätteen välille suoraa näköyhteyttä, mikä tekee menetelmän käyttämisestä häiriöaltista. (Tuominen 2003, 16.)

RFID

RFID-tiedonsiirto perustuu passiivisiin radiopiireihin. Tiedonsiirtoetäisyyden kantama voi olla lyhyt, muutamasta senttimetristä metrin pituuteen. Suurimpana vahvuutena RFID-teknologian käytössä on sen nopeus, sillä yhteyden muodostaminen onnistuu käytännössä välittömästi. Koska kantama on lyhyt, on erittäin epätodennäköistä, että kaksi eri RFID-piiriä pääsevät kommunikoimaan yhtä aikaa saman maksupäätteen kanssa. Kyseinen ongelma voi esiintyä varsinkin Bluetooth-tekniikan käytössä. (Tuominen 2003, 16.)

Lähimaksaminen voi Mobey Forumin tekemän analyysin mukaan perustua ainoastaan RFID-piiriin (NFC), koska muut ratkaisut ovat siihen nähden hitaampia ja epäluotettavampia (Tuominen 2003, 16). NFC on alun perin matkapuhelimia varten kehitetty lyhyen etäisyyden kommunikointitekniikka, joka perustuu HF RFID -teknologiaan (Seppä 2009, 6). Tätä teknologiaa esitellään luvussa 3.

Maksaminen etämaksumenetelmillä

Lähimaksamiseen käytetään nykyään edelleen myös maksuratkaisuja, jotka ovat alun perin suunniteltu selvästi etämaksamista varten. Tekstiviestillä ja puhelinsoitolla maksaminen ovat molemmat toimivia ratkaisuja, joten niiden käyttäminen on laajentunut vuosien kuluessa yhä laajempiin käyttökohteisiin. (Tuominen 2003, 5 - 8.)

Tekstiviestimaksamisessa voi esiintyä ongelmia tekstiviestien reaaliaikaisuuteen liittyen. Tekstiviestillä maksettaessa tekstiviestikeskuksien toiminta voi olla hidasta. Tämän vuoksi maksamisessa voi joissakin tilanteissa ilmetä ongelmia. (Tuominen 2003, 8.) Tekstiviestillä tai puhelinsoitolla maksaminen on joka tapauksessa työläämpää ja hitaampaa NFC-tekniikalla suoritettavaan lähimaksamiseen nähden.

3 NFC

NFC (Near Field Communication) on lyhyen etäisyyden kommunikointitekniikka, joka yhdistää laitteiden välisen tunnistamisen ja kommunikoinnin langattomasti. NFC-tuotteet ja -ratkaisut yksinkertaistavat ja nopeuttavat monien päivittäisten toimintojen suorittamista. (Sunsero 2012.) Kun NFC-matkapuhelimella kosketetaan esineitä, on mahdollista esimerkiksi kerätä ja välittää tietoa nopeasti, sekä käynnistää erilaisia palveluita. Tekniikan sovellutusmahdollisuudet ovat erittäin laajat. Sitä voidaan hyödyntää tiedonsiirron lisäksi esimerkiksi helpossa, nopeassa ja turvallisessa maksamisessa tai erilaisissa lipuissa. Maksamista varten matkapuhelimeen on mahdollista ladata käyttörahaa tai puhelin voi sisältää luottokorttiominaisuuden. (RFID Lab Finland ry 2012d.) Tekniikkaa pystytään hyödyntämään esimerkiksi älykorteissa, kiinnitettävissä tarroissa tai integroituna matkapuhelimen sisään. NFC:n vahvuuksiin voidaan lukea sen nopeus ja helppous, sekä hyödyntämisen lukuisat käyttömahdollisuudet. (NFC-työryhmä 2010, 4 - 5.)

NFC-tekniikassa käytetään HF-taajuusalueelle sijoittuvaa 13,56 MHz:n taajuutta, jonka lukuteho on rajattu standardissa siten, että lukeminen onnistuu korkeintaan 4 senttimetrin pituiselta matkalta. Lukulaitteen signaali on tästä huolimatta mahdollista kuulla jopa metrin päähän. (Seppä 2011, 11.) Perinteisistä RFID-laitteista poiketen NFC-laitteet pystyvät toimimaan sekä tunnisteena, että lukulaitteena. Tämä tekee mahdolliseksi esimerkiksi RFID-kommunikoinnin kahden matkapuhelimen välillä. (Seppä 2009, 17.)

NFC:n muisti vaihtelee käyttötarkoituksesta riippuen sadoista biteistä jopa miljooniin bitteihin asti. Jotta päästään nopeuksiin, joissa jopa videon siirtäminen onnistuu passiivisesta etätunnisteesta matkapuhelimeen, on yhdistettävä esimerkiksi UHF-tekniikan energiansyöttö ja laajakaistainen UWB-tiedonsiirto tunnisteesta lukijalle. (Seppä 2011, 11.)

Seuraavassa luvussa käydään läpi tarkemmin RFID-tekniikkaa, johon NFC:n toiminta perustuu.

3.1 RFID

RFIDllä (Radio Frequency IDentification) tarkoitetaan radiotaajuista etätunnistusta, joka perustuu tunnisteiden ja lukijalaitteen väliseen kommunikointiin. Tähän käytetään radioaaltoja. RFID-tunnisteet ja lukijat luokitellaan radiolaitteiksi, koska ne tuottavat ja heijastavat sähkömagneettista säteilyä. Niiden on toimittava tarkasti rajatuilla radiotaajuuksilla ja suurin sallittu säteilyteho on rajoitettu. (VISI RFID Solutions Oy 2012.)

Sirut mahdollistavat monet tämänpäiväiset mukavuudet. Jos esimerkiksi työpaikalla vaaditaan kulunvalvontakorttia, mahdollistaa siru työpaikalla liikkumisen. Myös autossa voi olla laite, joka maksuportin läpi ajettaessa maksaa automaattisesti vaaditun tiemaksun. RFID-siruja käytetään nykyään yhä enemmän maksujärjestelmissä niiden helppouden vuoksi. Korttia ei tarvitse asettaa enää lukulaitteeseen, vaan maksu hoituu kätevästi heilauttamalla esimerkiksi lompakkoa tai avaimenperää lukulaitteen yli. RFID-sirut pienenevät ja muuttuvat entistä edullisemmiksi, mikä mahdollistaa niiden käytön laajentamisen. (Foley 2012.) Sepän (2009, 8) mukaan RFID on ollut 2000-luvun ensimmäisellä vuosikymmenellä samassa tilanteessa, jossa matkapuhelimet olivat 20 vuotta sitten. Kasvu jatkuu huimaa vauhtia eteenpäin.

Etätunniste on tiedonvaihtomenetelmä, joka perustuu heijastusperiaatteeseen:

> ”Lukulaite lähettää kantoaallon tai moduloidun kantoaallon ja vastaanottaa samaan aikaan tai välittömästi moduloinnin jälkeen etätunnisteen heijastamaa signaalia. Lähettimen modulaatio on aina amplitudimodulaatiota, mutta etätunniste voi moduloida joko amplitudia tai vaihetta. Lukulaitteeseen saapuva heijastuneen signaalin taajuus on sama kuin lähetetyn signaalin, joten ilmaisussa voidaan käyttää vaihelukitustekniikkaa. Se puolestaan parantaa signaali-kohinasuhdetta eli vähentää kohinaa ja häiriöiden vaikutusta merkittävästi.” (Seppä 2009, 9.)

Nykyaikaisia RFID-tunnisteita ei tulisi verrata viivakoodeihin, joita luetaan yleensä laserilla ja joista tarkastellaan vain signaalin valon heijastunutta tehoa (Seppä 2009, 9). Parempana vertailukohteena voidaan pitää radiota, jolta onnistuu tiedon kerääminen, prosessointi ja salaaminen. Se voi myös sisältää muistia musiikkikappaleen verran. (Seppä 2011, 8.) Toisin kuin radio, RFID-lukulaite lähettää kantoaaltoa samalla kun se myös vastaanottaa modulaatiota, joka heijastuu kohteen etätunnisteesta (Seppä 2009, 9). Etätunnistamisen toteuttaminen onnistuu myös optisesti viivakoodilla. Lisäksi voidaan käyttää matriisikoodausta, jonka yleistymiseen ovat myötävaikuttaneet matkapuhelinten kamerat. (Seppä 2011, 8.)

RFID:stä ei ole uhkaa viivakoodille ainakaan lähitulevaisuudessa. Viivakoodin ja RFID:n hyödyt ovat osaksi päällekkäisiä, mutta myös erillisiä. Viivakoodi on RFID:tä edullisempi käyttää kohteissa, joissa RFID:n hyötyjä ei erityisesti tarvita. RFID toimii viivakoodia paremmin esimerkiksi silloin, kun tunnisteen lukeminen halutaan tehdä kaukaa, halutaan tehdä useampia lukutapahtumia samanaikaisesti, tunniste halutaan piilottaa tai siihen ei onnistuta saamaan muuten näköyhteyttä, tunnistaminen tapahtuu ympäristössä, jossa tunniste altistuu lialle tai jossa siihen kohdistuu voimakasta kulumista. Viivakoodin tietosisältö on tulostamisen jälkeen muuttumatonta, toisin kuin RFID-tunnisteessa, jossa tietosisältö voi olla myös dynaamista. (RFID Lab Finland ry 2012e.) Kaupat ovat ryhtyneet ottamaan tuotteiden yksilöimistä varten käyttöönsä usean perinteisen viivakoodin yhdistelmän. Laajennetut viivakoodit tulevat yleistymään nopeasti, koska kaupan laserpohjaiset lukulaitteet voivat lukea näitä koodeja. (Seppä 2011, 8.)

3.1.1 Taajuusalueet

Tunniste ja lukija keskustelevat keskenään käyttäen aina juuri tiettyä taajuutta (RFID Lab Finland ry 2012b). Kun taajuus on etätunnistimen ja lukijan väliseen etäisyyteen nähden matala, on kyseessä niin sanottu lähikenttätilanne. Muussa tapauksessa on kyse säteilykentästä. Etätunnistimet jaetaan eri luokkiin myös käytettävän taajuuden mukaan. (Seppä 2011, 10.) Taajuusalueiden käyttämistä ja säteilytehoja kontrolloi Suomessa Viestintävirasto. Lisäksi Eurooppalainen telealan standardisoimisjärjestö ETSI (European Telecommunications Standards Institution) on luonut standardeja, joita hyödyntäen eri valtioiden viranomaiset, jotka vastaavat valtion telekommunikaatiosta, voivat luoda eri taajuusalueiden käyttämisestä omat kansalliset säädöksensä. Taajuusalueiden luominen on tärkeää, jotta RFID-laitteistot eivät aiheuta häiriötä niihin sovelluksiin ja laitteisiin, jotka hyödyntävät muita radioaaltoja. Tällaisia ovat esimerkiksi televisio- ja radiolähetykset, teollisuuden tuotantolaitteet, sekä viranomaisten käyttämät radioviestimet. (VISI RFID Solutions Oy 2012.) Keskusteluun valjastettu fysikaalinen mekanismi voi olla erilainen eri taajuusalueilla. LF- ja HF-taajuusalueilla käytetään induktiivista kytkentää, mutta UHF- ja mikroaaltotaajuuksilla on kyse radioaalloista. (RFID Lab Finland ry 2012b.) Käytössä olevat taajuusalueet voidaan jaotella eri ryhmiin seuraavasti:

LF (Low Frequency)

Järjestelmät toimivat taajuusalueella yleisimmin 125 kHz:n taajuudella. LF-järjestelmien käyttö rajoittuu nykyaikana enää tiettyihin sovelluksiin, joita käytetään kulunvalvontaan ja eläintunnistukseen. (RFID Lab Finland ry 2012b.)

HF (High Frequency)

Käytännön standarditaajuus on 13,56 MHz. Taajuus on kansainvälisesti vapaa. HF-taajuutta hyödyntäviä järjestelmiä käytetään yleensä lähietäisyydellä tapahtuvassa tunnistamisessa, esimerkiksi kulunvalvonnassa. HF-järjestelmillä on myös uusia käyttökohteita ja vielä nykypäivänäkin tämä on hyvin käyttökelpoinen taajuus. Optimiolosuhteissa 13,56 MHz:n pisin lukuetäisyys sirun ja antennin välillä on suunnilleen 1,5 metriä. Lukuetäisyydet vaihtelevat käytännössä sovelluksen mukaan 0,05 ja 1 metrin välillä. HF-taajuuden etuna voidaan pitää

UHF:n verrattuna ainakin kentän parempaa läpäisykykyä aineisiin, jotka sisältävät vettä. Tällaisia ovat esimerkiksi ihmiskeho tai puutuotteet. Lisäksi taajuus sietää paremmin teollisuusympäristön häiriöitä, lukualue on helppo rajata, eikä heijastuksen suhteen ole ongelmia. (RFID Lab Finland ry 2012b.)

UHF (Ultra High Frequency)

Tällä taajuusalueella toimivat RFID-järjestelmät ovat vielä tällä hetkellä keksintönä kohtalaisen uusi. UHF-alueella taajuudet hieman vaihtelevat ympäri maailmaa. Yhdysvalloissa taajuusalue voi olla 902 - 928 MHz, mutta eurooppalainen sallittu taajuusalue on noin 869 MHz. UHF-tekniikka herättää mielenkiintoa eniten sen mahdollisuuksista logistiikan sovelluksissa. Tunnetuissa maailmalla toimivissa logistiikan toimitusketjuihin liitetyissä RFID-lukijoissa sovelletaan juuri UHF-tekniikkaa (esimerkiksi Metro Group, Wal-Mart). HF ja LF RFID-tunnistuksessa on kyse ”near-field” induktiivisesta kytkennästä, jossa tunnisteen on tarkoitus reagoida lukijan oskilloivaan (värähtelevään) magneettikenttään. UHF RFID-tunnistuksessa on kyseessä tekniikka, jota kutsutaan nimellä ”far-field”. Tässä tekniikassa tunniste ja lukija kommunikoivat lähettämällä sähkömagneettista säteilyä (radioaaltoja). UHF-tekniikkaa voidaan verrata radioon, kun taas LF- ja HF-tekniikka toimii kuin muuntaja. (RFID Lab Finland ry 2012b.)

UHF-tekniikka tuo rajoitteita nesteiden ja metallien läheisyydessä, mutta taajuudelle on kehitetty tätä varten lähikenttä UHF-tunnistaminen (Near Field UHF), jossa käytetään UHF-taajuudellakin olevaa lähikenttää, joka ylettyy noin 20 senttimetrin etäisyydelle. Tässä magneettikenttä on tunnistamista varten riittävän vahva. Lähikenttä UHF toimii UHF-lukijalla ja tarkoitukseen erityisesti kehitellyllä lähikenttä antennilla. Tunnisteissa, jotka toimivat lähikentässä, on yksi antennisilmukka ja UHF-mikrosiru. Lukuvarmuus nesteiden ja metallien läheisyydessä on magneettikentän ansiosta parempi kuin tavallisessa UHF-tekniikassa, joka perustuu kaukokenttään. Myös antenni on edullisempi ja pienikokoisempi. (RFID Lab Finland ry 2012b.)

Mikroaallot

Yleisin taajuus mikroaaltoalueella on 2,4 GHz. Enimmäkseen mikroaaltoja käytetään aktiivitunnistuksessa, jossa tunnisteen sisällä on oma virtalähde. Tunnettu mikroaaltoja hyödyntävä sovellus on esimerkiksi tietullien käyttämä automaattinen tunnistus. (RFID Lab Finland ry 2012b.)

Tällä hetkellä kaikkein tärkeimmät ja eniten kasvavat teknologiat ovat passiiviset HF- ja UHF-teknologiat sekä NFC. HF- ja UHF-tunnisteiden merkitys on kasvanut viimeaikoina niille rakennettujen standardien ansiosta. Molemmille tunnisteille on löydetty paljon mahdollisia käyttökohteita. Kehitys on laittanut yritykset hakemaan standardien avulla kyseisille tekniikoille yleistä hyväksyntää. Foorumina standardoimisessa on ollut suurimmaksi osin ISO ja näiden päälle on rakennettu UHF:lle EPC (Electronic Product Coding) ja Gen2 sekä HF:lle esimerkiksi NFC (Near Field Communication). (Seppä 2011, 10.) Taulukossa 3 havainnollistetaan eri taajuusalueiden lukuetäisyyksiä, tärkeimpiä käyttökohteita, sovellutusvuosia, edullisimpia hintoja, sekä nykyistä tilannetta standardoinnin suhteen.

Taulukko 3. RFID:n taajuusalueet (Seppä 2009, 13).

Taajuus	Etäisyys	Sovellutus	Sovellutus-vuosi	Hinta	Standardit
LF	0,1 m	Avaimet/tehdas-automaatio	1980 -	0,2 €	Ei ole
HF	0,5 m	Liput/Tuotanto-automaatio	1995 -	0,05 €	ISO/NFC
UHF	5,0 m	Logistiikka	2003 -	0,03 €	ISO/EPC

Uusia taajuuksia ja viranomaismääräyksiä on tulossa kokoajan lisää ja standardoimisprosessit ovat vielä osittain kesken. Standardoimistyö on kesken erityisesti RFID-antureihin liittyen, mutta tämä ei kuitenkaan estä alan kehittymistä, koska tiedonsiirto hoidetaan myös RFID-antureissa hyödyntäen joko HF/NFC- tai EPC-standardeja. HF:n (myös NFC:n) osalta on oleellista, että sama taajuus on käytettävissä kaikkialla maailmassa. Tästä poiketen UHF:llä on poikkeavat taajuudet jokaisessa maanosassa. Laajakaistainen antenni pystyy toimimaan koko taajuusalueelle kohtuullisesti, mutta siirtolinjatyyppiset, matalat metallin

päällä toimivat antennit ovat niin kapeakaistaisia, että niitä ei saada toimimaan kaikilla mantereilla ilman hajaviritystä. Kiinassa ollaan ottamassa käyttöön kaksi taajuutta, yksi lähelle Eurooppaa ja toinen USA:n taajuusaluetta. Eurooppa on myös tuonut taajuuden USA:n taajuuden sisälle. Näiden toimenpiteiden avulla helpotetaan UHF-alueella globaalisten etätunnistimien soveltamista. (Seppä 2011, 10.)

3.1.2 Standardit

Standardit ovat tärkeitä RFID-tekniikkaan liittyen varsinkin logistiikan sovelluksissa, joissa rakennetaan avoimia kuljetusketjuja. Tällöin useiden eri toimijoiden on pystyttävä lukemaan samoja tunnisteita eri järjestelmistä huolimatta. Standardien on myös taattava valmistajariippumattomuus. Kun rakennetaan isoa järjestelmää, on hyvä varmistaa, että sopivia laitteita ja tunnisteita voi ostaa myös myöhemmin vapaasti ilman, että on tarvetta sitoutua tiettyyn toimittajaan. Standardit eivät sinänsä takaa, että järjestelmästä tulisi valmistajariippumaton. Osa standardeista on kuitenkin vapaita, joiden mukaisesti kuka tahansa voi ryhtyä valmistamaan laitteistoja. (RFID Lab Finland ry 2012f.)

Standardit liittyvät RFID-tekniikassa mahdollisesti moneen asiaan. Tärkeimmät standardit määräävät, mitä tiedonvälitysprotokollaa käytetään ja mitä tietosisältöä tunnisteessa on. (RFID Lab Finland ry 2012f.) Alla on esitelty yleisimmät standardit taajuusalueittain.

LF-taajuusalue

Alueella ei ole vapaita standardeja. Suurin osa sovelluksista on toteutettu 125 kHz:n taajuudella suljettuina järjestelminä. Eläinten tunnistuksessa käytetään ISO11784-standardia, joka määrää mitä tietosisältöä tunnisteeseen laitetaan ja ISO11785 määrittelee 134 kHz:n taajuudella olevan tiedonsiirtoprotokollan. (RFID Lab Finland ry 2012f.)

HF-taajuusalue

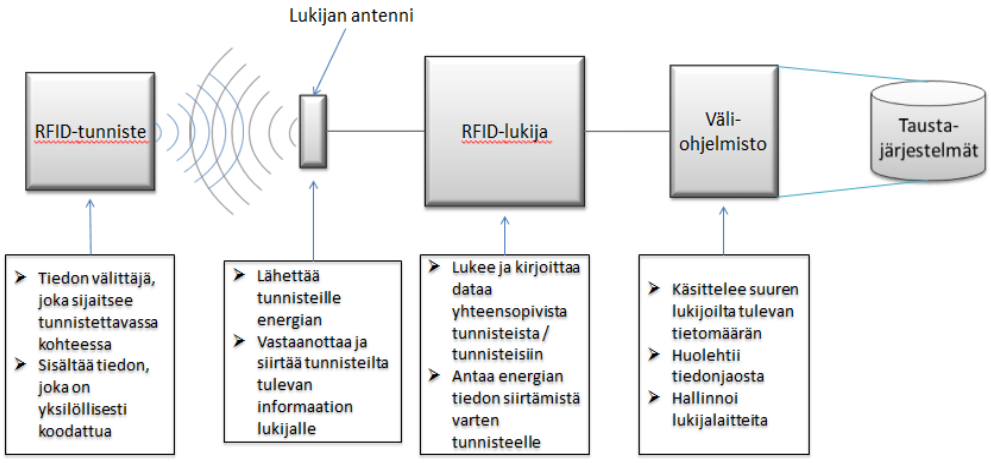
Sovittuja standardeja 13,56 MHz:n taajuudella. ISO14443-standardi (proximity cards) ei takaa tunnisteiden ja lukijoiden yhteensopivuutta valmistajariippumattomasti, joten se ei tuo kaikkia standardien etuja. Philips Mifare -tekniikka on käytännössä saavuttanut aseman de facto -standardina. Mifare-tekniikkaa käytetään maksusovelluksissa 3 - 4 senttimetrin lukuetäisyydelle rajattuna. ISO15693-standardi (vicinity cards) on valmistajariippumaton. ISO15693-standardia noudattaa suomessa tunnetuimpana I-CODE SLI -siru. Vanhempi versio tästä on Philips I-CODE, joka myös on edelleen käyttökelpoinen. (RFID Lab Finland ry 2012f.)

UHF-taajuusalue

Olennaisin standardi on tällä hetkellä ISO18000-6C, eli toisin sanoen Class 1 Gen 2, joka on EPC Global -järjestön kehittämä protokollastandardi. Kyseisen standardin myötä UHF-taajuuden tunnistus on varmempaa ja toimintaa monilukijaympäristössä on saatu paranneltua. (RFID Lab Finland ry 2012f.)

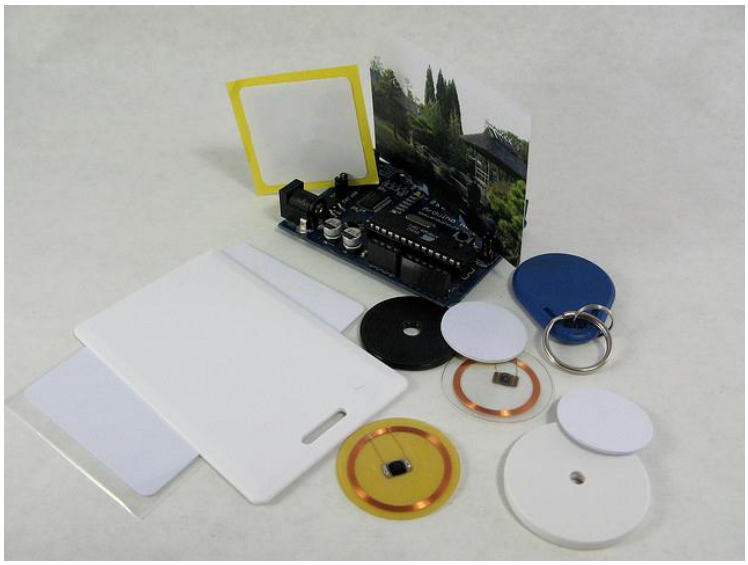
3.1.3 RFID-komponentit

RFID-järjestelmä tarvitsee tiedonsyöttämistä, lukemista ja hyödyntämistä varten tunnisteen, lukijalaitteen ja taustajärjestelmän (Logimek Oy 2012). Kuvassa 3 havainnollistetaan RFID-järjestelmän toimintaa.



Kuva 3. RFID-järjestelmään kuuluvat komponentit (RFID Lab Finland ry 2012g).

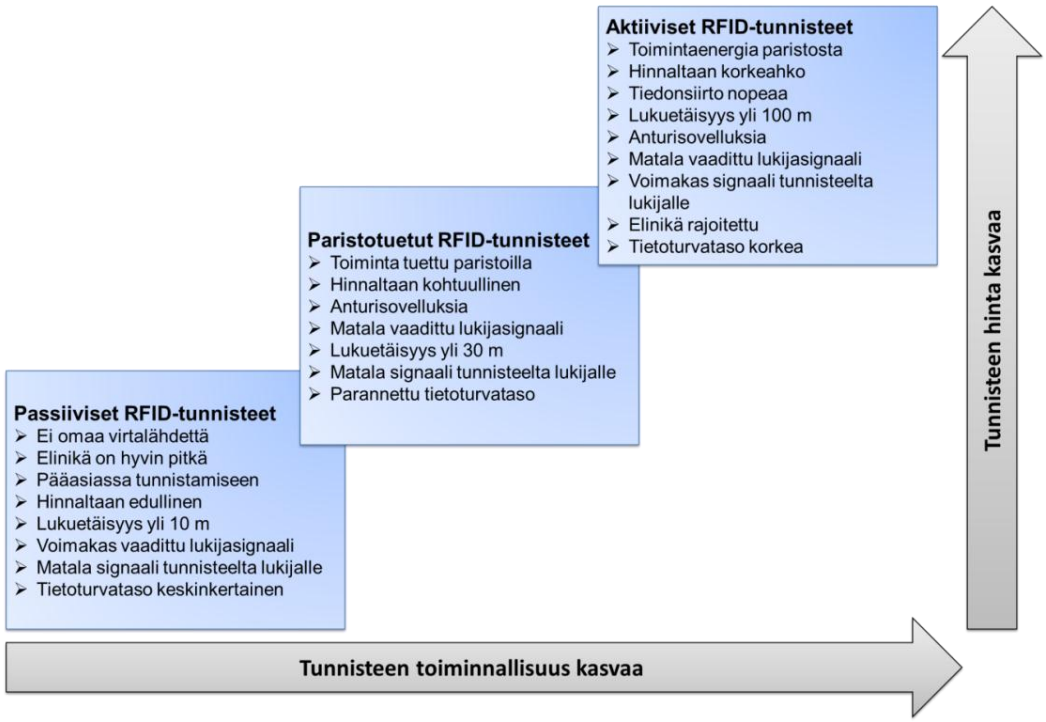
Tunniste voi olla esimerkiksi tarra, nappi, lappu, kortti tai implantti (kuva 4). Sen sisällä on antenni ja tiedon säilyttämiseen tarkoitettu siru. Tunnisteella on kiinteä sarjanumero ja vapaata kirjoitustilaa standardista riippuen. Yleensä tunnisteeseen on kirjoitettu vain sen yksilöivä sarjanumero (EPC, Electronic Product Code). (RFID Lab Finland ry 2012g.) Tunniste on mahdollista sijoittaa valmistusvaiheessa tuotteen sisään, jolloin se on poissa näkyvistä (Logimek Oy 2012).



Kuva 4. Erilaisia RFID-tunnisteita. (Kuva: Tod Kurt.)

RFID-tunnisteet jaetaan tyypillisesti passiivisiin, semipassiivisiin ja aktiivisiin etätunnisteisiin. Passiivisessa etätunnisteessa ei ole erillistä virtalähdettä. Tällöin tunnisteen tarvitsema energia otetaan lukijalaitteen synnyttämästä kentästä. Semipassiivisen etätunnisteen sisällä on oma virtalähde (patteri tai akku), jonka ansiosta lukuetäisyys voi olla pidempi, eikä toimintaan tarvita lukulaitteen tuottamaa energiaa. Semipassiivinen tunniste ei voi lähettää tietoa radioteitse ilman lukulaitetta, sillä se ei ole itsenäinen radio. Kun RFID-tunnisteisiin lisätään antureita, lisääntyy semipassiivisten tunnisteiden rooli entisestään. Näitä voidaan hyödyntää valvottaessa kiinteistöjen ja rakenteiden kuntoa, logistisen ketjun laatua, sekä tulevaisuudessa yhä enemmän ihmisten terveydentilaa. (Seppä 2011, 9.) Semipassiiviset etätunnisteet tulivat käyttöön ensin, mutta nykyään etätunnisteista yhä suurempi osa on passiivisia niiden kasvaneen merkityksen myötä. Molempia tekniikoita sovelletaan jatkossakin, mutta passiivisten etätunnisteiden käyttömäärä on satoja kertoja suurempi. (Seppä 2009, 9.)

Kuvassa 5 vertaillaan tunnisteiden toiminnallisuutta. Toiminnallisuuden kasvaessa myös hinta kasvaa rajoittaen kalliiden tunnisteiden käyttöä.



Kuva 5. Passiivisten, semipassiivisten ja aktiivisten tunnisteiden toiminnallisuuden vertailua (RFID Lab Finland ry 2012g).

Varsinainen tieto noudetaan taustajärjestelmän tietokannasta. RFID-lukija lukee ja laitteesta riippuen myös kirjoittaa tunnisteen sisältöä. Kohteeseen ei tarvita fyysistä kontaktia tai näköyhteyttä. Lukuetäisyyksiin vaikuttaa taajuusalue ja standardi. (RFID Lab Finland ry 2012g.) Logimek Oy:n mukaan lukulaitteita voivat olla OEM-moduulit (älykkäisiin laitteisiin sijoitettavat luku ja kirjoitusyksiköt), lähilukijat, jotka kytketään yleensä USB tai RS-232-liitännällä (lukuetäisyys noin 10 senttimetriä), reaaliaikaisella tai keräävällä toiminnolla toimivat langattomat tiedonkeruulaitteet (lukuetäisyys noin 10 senttimetriä), Mid Range -lukijat, jotka kytketään yleensä USB tai RS-232-liitännällä (Lukuetäisyys alle 50 senttimetriä), sekä long Range -lukijat ja portit, joiden läpi kuljetetaan tuotteita tai kävellään. Nämä kytketään yleisesti USB, Ethernet tai RS-232-liitännällä (lukuetäisyys alle 1,5 metriä). Taustajärjestelmässä lukijalaitteille tarvitaan hyödynnettävät kaapelit ja ohjelmistot, tiedonkeruu- ja käsittelyohjelmisto, kytkennät nykyiseen tietojärjestelmään, sekä tarvittaessa langattomat siirtotiet. (Logimek Oy 2012.)

3.1.4 Etätunnistepiirit

RFID-teknologian merkitys lyhyellä etäisyydellä kommunikoitaessa on kasvanut hyvin suureksi ja kasvaa edelleen voimakkaasti. Tähän on vaikuttanut merkittävästi juuri edullisuus ja mahdollisuus toimia ilman erillistä teholähdettä. Radio, joka toimii heijastusperiaatteella, voidaan toteuttaa kokoluokan 0.25 mm^2 piirisirulla, joka on CMOS-pohjainen. Piirisiru on mahdollista valmistaa prosessilla, jossa viivanleveys on 0.35 - 0.6 µm. Tämä prosessi on jo hieman vanhanaikainen, joten puolijohdevalmistajat voivat hyvin käyttää valmistamiseen edelleen vanhoja tuotantotilojaan ja laitteitaan. Tällaisen piirisirun valmistuskustannukset ovat edullisimmillaan 0,01 sentin luokkaa. Etätunnistimen edellyttämä antenni ja tarralaminaatti nostavat hintaa edullisimmillaan noin 0,03 senttiin. Markkinahinta on tällä hetkellä suurina erinä noin 0,05 senttiä. (Seppä 2011, 9.)

Antenni vaikuttaa etätunnistimen kokoon. Pitkän lukuetäisyyden tunniste on aina suuri ja tässä mielessä myös aina havaittavissa (koko vähintään 1 x 3 cm). HF-tunnisteet ovat pienimmillään noin 2,5 x 2,5 cm. Etätunniste on mahdollista tehdä myös hyvin ohueksi (0,1 mm), mikä mahdollistaa tunnisteen piilottamisen tuotteeseen huomaamattomasti. RFID-tunnisteita on asennettu viimeaikoina myös ihmisten ihon alle, mutta antennin pienuudesta johtuen niiden lukeminen vaatii lähes ihoon koskettamista. (Seppä 2011, 9.)

Etätunnisteen sisältämää tietoa on mahdollista lukea ja muuttaa langattomasti. Kun valmistetaan standardin mukainen mikropiiri, on siinä aina jälkeenpäin muuttumaton pysyvä muisti. Tämän vuoksi kahta samanlaista etätunnistetta ei periaatteessa ole olemassa. Yritys voi kirjoittaa hyödyntämäänsä tunnisteeseen yksikäsitteisen lukitun koodin. Kiinteästi ohjelmoitavan koodin pituus on sitä suuruusluokkaa, että jokainen maailmassa ikinä valmistettu tuote voidaan merkitä erillisellä koodilla. Piiri sisältää usein muistia, joka on uudelleenkirjoitettavissa. Tämä muisti vaihtelee sovelluksesta riippuen. Jotta muistia pääsee lukemaan ja kirjoittamaan, tarvitaan aina salasana ja tiedon kryptaus. Salauksen turvataso vaihtelee aina sen mukaan, mistä standardista ja sovellutuksesta on milloinkin kyse. (Seppä 2011, 9 - 10.)

3.1.5 RFID:n käyttökohteita

RFID-sirut mahdollistavat monet nykyajan mukavuudet. Ne esimerkiksi päästävät paikkoihin (kulunvalvonta), merkitsevät kohteita, lisäävät turvallisuutta (esimerkiksi liikenteessä), sekä helpottavat maksutapahtumaa, tiedon löytämistä ja jakamista. (Foley 2012.)

RFID:tä käytetään tällä hetkellä laajasti ainakin tuotantoautomaatiossa, logistiikassa, lentokoneiden tutkavalvonnassa, kulunvalvonnassa, auton avaimissa, liputtamisessa (metrot ja linja-autot), eläinten merkitsemisessä, henkilökorteissa ja passeissa, sekä vaatteiden merkitsemisessä. Lisäksi RFID:tä hyödynnetään pienemmissä sovellutuskohteissa, kuten parkkeerauksessa, sairaaloiden henkilökunnan ja potilaiden tunnistamisessa, lääkkeiden alkuperäistunnistuksessa, pesuloissa, sekä lentoliikenteen matkalaukuissa. (Seppä 2011, 16.)

Teknologiaa tullaan hyödyntämään tulevaisuudessa yhä enemmän myös matkapuhelimella maksamisessa ja liputtamisessa, ohjelmistojen lataamisessa matkapuhelimeen, avaimissa, kaupan hintalappujen yhteydessä olevassa tuoteinformaatiossa, kauppojen ja tuotteiden hyödyntämisessä, lääkepakkauksissa, kuluttajatuotteissa, merkittäessä kulkuneuvojen osia, varastetun ajoneuvon seurannassa, nopeuden valvonnassa, aktivoitaessa palveluita, lentoliikenteessä (matkaliput) ja lentokoneiden kriittisten komponenttien hallinnoimisessa, kiinteistöjen seinien ja betonivalujen kosteutta mittaavissa antureissa, siltojen, rakennuksien ja lentokoneiden rakenteiden valvonnassa, kylmäkuljetuksien (myös muiden) laadunvalvonnassa, sekä pitkän lukuetäisyyden kulunvalvonnassa. (Seppä 2011, 16 - 17.)

Asiantuntijoiden mukaan ei ole mahdoton ajatus, että vielä jonakin päivänä asiakas voi poistua ostoksilta supermarketista ilman, että RFID-sirulla varustettuja ostoksia tarvitsisi enää viedä kassalle laskettavaksi. Tällöin ostokset veloitetaan antennin ohi käveltäessä suoraan RFID-sirulla varustetulta luottokorttitililtä. (Foley 2012.) Luultavasti tämä myös samalla vähentäisi radikaalisti myymälävarkauksien määrää.

3.2 NFC:n toimintamoodit

NFC-laitteet ovat ainutlaatuisia siinä, että ne voivat toimia sekä tunnisteena että lukijalaitteena (NFC-työryhmä 2010, 2). NFC-laitteet voivat muuttaa toiminta-moodiaan kortin emulointi -moodiin, luku/kirjoitus-moodiin, tai laitteelta toiselle laitteelle -moodiin. Toimintamoodit perustuvat kontaktittomien älykorttien standardeihin ISO/IEC 18092, NFC IP-1 ja ISO/IEC 14443. (Aarinen 2006, 3.)

Kortin emulointi

Kortin emulointi -moodissa NCF-laite toimii tunnisteena. Laite näyttää ulkoiselle lukijalle samanlaiselta kuin normaali kontaktiton älykortti. (Aarinen 2006, 3.)

Kortin emuloinnin käyttökohteita ovat esimerkiksi matkakortit, henkilökortit, liput, kupongit, pankkikortit, luottokortit, kanta-asiakaskortit, sekä voucherit. Moodi mahdollistaa myös kortti-informaation käyttöliittymän ja sovelluksen käyttäjälle. (Suikkanen 2011a, 4.)

Luku/kirjoitus

Tässä moodissa NFC-laite osaa lukea ja kirjoittaa RFID ja NFC -tunnisteita ja -kortteja. Tunniste voi sisältää esimerkiksi tunnisteen ID:n, SMS-viestin lähetys- tai soittamistoiminnon johonkin numeroon, jonkin sovelluksen käynnistämistoiminnon, linkin internetsivulle tai kontaktitietoja. (Suikkanen 2011a, 5.)

Luku/kirjoitus -moodin käyttökohteita ovat esimerkiksi informaation tai palvelun hakeminen, käyttäjän tai paikan tunnistaminen, ylläpitoprosessit ympäristössä, sekä erilaisten palveluiden toteuttaminen (Suikkanen 2011a, 5).

Laitteelta toiselle laitteelle

Tässä toimintamoodissa kahden NFC-laitteen välille luodaan yhteys, jolloin ne voivat vaihtaa keskenään tietoa. Moodin standardointi löytyy ISO/IEC 18092 -standardista. (Aarinen 2006, 3.)

NFC-yhteyden avulla tiedostojen jakaminen onnistuu helposti matkapuhelinten kesken, kun ensin etsitään jaettava tiedosto ja tämän jälkeen vain kosketetaan

matkapuhelinta, johon tiedosto halutaan lähettää. Ainoana toimintavaatimuksena on, että NFC löytyy tuettuna molemmista matkapuhelimista. (Nokia 2012.) Laitteiden välillä voidaan siirtää esimerkiksi kuvia, videoita tai ääniä, yhteystietoja, erillisen sovelluksen tietoja, sekä suorittaa todennus jollekin verkkoyhteydelle (WLAN, Bluetooth). (Suikkanen 2011a, 6.)

3.3 NFC-tuotteet

NFC-teknologia voi löytyä matkapuhelimesta tai muusta NFC-laitteesta. Teknologiaa hyödynnetään laitteiden lisäksi myös erilaisissa tunnisteissa, joita on olemassa erittäin laajat valikoimat erilaisiin käyttökohteisiin eri muodoissa ja erilaisilla ominaisuuksilla varustettuina. Matkapuhelinten lisäksi myös niin sanottujen NFC-älykorttien odotetaan yleistyvän lähiasioinnin, kuten juuri maksamisen välineenä. Myös lukulaitteita löytyy laajat valikoimat erilaisiin käyttötarkoituksiin.

3.3.1 NFC-ominaisuus matkapuhelimessa

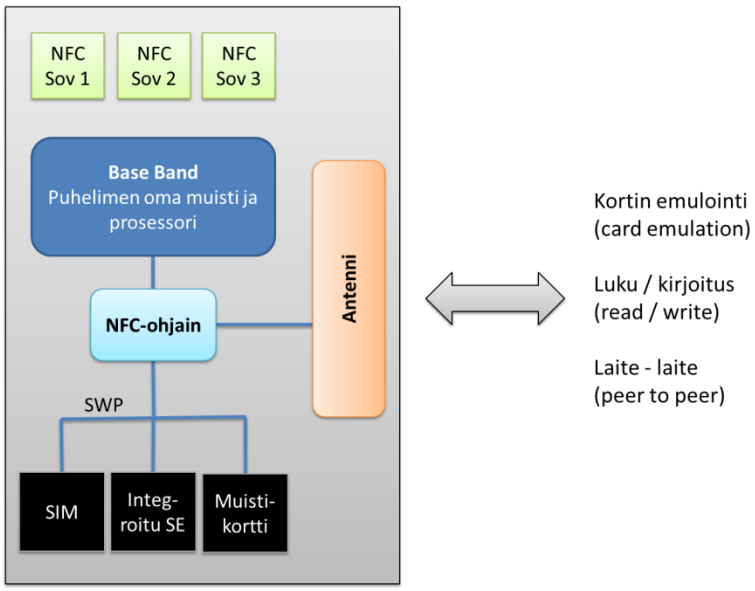
NFC-ominaisuus voi sijaita matkapuhelimessa integroituna, tai se voidaan lisätä jälkeenpäin puhelimen takakanteen liimattavalla NFC-tarralla. Tulevaisuudessa on mahdollista, että maksuominaisuus saadaan lisättyä matkapuhelimeen myös NFC-ominaisuuden sisältävällä SIM-kortilla. NFC-teknologia kehittyy edelleen, joten myös muut ratkaisut ovat tulevaisuudessa hyvin mahdollisia. Esimerkiksi SD-muistikortti voi tulevaisuudessa toimia NFC-sirun yhtenä mahdollisena sijoituspaikkana.

NFC integroituna matkapuhelimessa

NFC-matkapuhelimen avulla on mahdollista muodostaa yhteys muiden puhelimien, laitteiden ja vuorovaikutteisten tunnisteiden kanssa, sekä toimia näiden kanssa yhdessä. Yhteyden muodostamiseen riittää toisen laitteen tai tunnisteen koskettaminen. (Nokia 2012.)

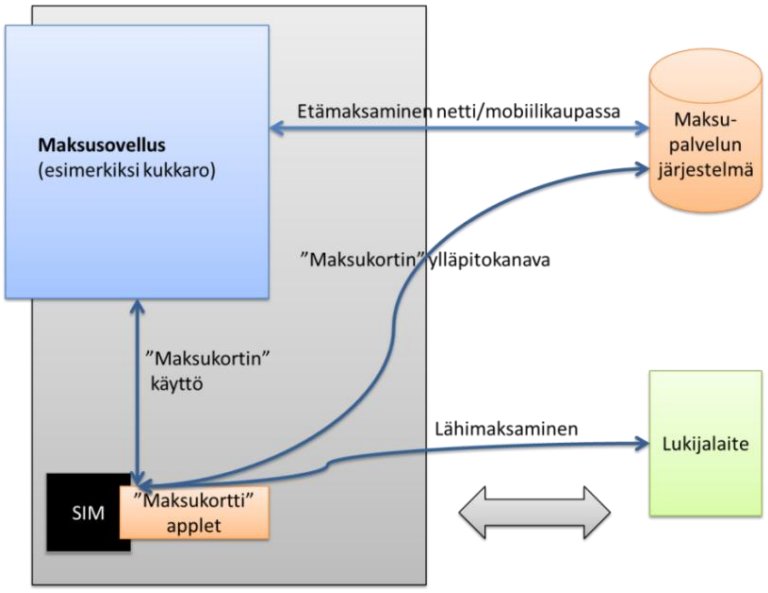
Puhelin, josta NFC löytyy integroituna, sisältää RFID-lukijan ja tunnisteen (RFID Lab Finland ry 2012d). NFC-ominaisuus voi sijaita matkapuhelimessa itsessään tai siinä käytettävässä SIM-kortissa (Luottokunta 2012b). Kaikki NFC-matkapuhelimet eivät tue NFC-maksamista, vaan esimerkiksi maksu-, lippu- ja avainsovelluksia varten laitteesta on löydyttävä siltä vaaditut tekniset ominaisuudet. Esimerkiksi matkapuhelimen, lukijalaitteen sekä tunisteen antennien kokosuhteella ja yhteentoimivuudella on suuri merkitys. (Suikkanen 2011a, 8 - 10.) Matkapuhelimesta tulee löytyä myös älysiru, jota kutsutaan turvaelementiksi (Secure Element). Turvaelementti mahdollistaa matkapuhelimen tallentaa turvallisesti maksuohjelman sekä käyttäjän tilitiedot ja käyttää näitä tietoja toimiessaan kuten maksukortti. NFC-maksutapahtumat maksupäätteen ja matkapuhelimen välillä käyttävät ISO/IEC 14443 -standardin kommunikointiprotokollaa tietojen välitykseen. (Smart Card Alliance 2012.) Turvaominaisuuksien sijoittaminen on aiheuttanut laitevalmistajien ja operaattorien kesken erimielisyyksiä, mutta asiassa on päästy sopimukseen siitä, että turvaominaisuuden paikka on puhelimen SIM-kortilla. Paikka on paras vaihtoehto mobiilimaksamisen käytön ja toiminnallisuuden kannalta. SIM-kortin toimitusketjun vaatimuksien kasvaminen asettaa operaattoreille uuden haasteen turvallisuuden takaamisesta. (RFID Lab Finland ry 2012d.)

Kuvassa 6 havainnollistetaan NFC:n toimintaa matkapuhelimessa. Sisältä löytyy SIM-kortti, integroitu turvaelementti (SE) sekä muistikortti. Antenni lähettää ja vastaanottaa tietoa.



Kuva 6. NFC matkapuhelimessa (Suikkanen 2011a, 7).

Matkapuhelinta on mahdollista käyttää erilaisissa toimintamoodeissa, joita ovat kortin emulointi, luku/kirjoitus sekä laitteelta toiselle laitteelle tapahtuva tiedon siirto. Maksamista varten matkapuhelimeen voidaan tarvita myös oma maksusovellus, jonka toimintaa havainnollistetaan kuvassa 7.



Kuva 7. Maksusovellus matkapuhelimessa (Suikkanen 2011a, 17).

Maksutapahtumassa ostoksen vahvistuspyyntö ja maksaminen (vahvistus) matkapuhelimen ja lukijalaitteen välillä tapahtuu NFC-tiedonsiirrolla. Käyttö- ja palveluprosessit ovat vielä tällä hetkellä määrittelyvaiheessa (EMVCo, pankit, operaattorit). (Suikkanen 2011a, 18.)

Esimerkiksi MasterCard kertoo verkkosivuillaan, kuinka NFC-maksaminen onnistuu MasterCard PayPass® -palvelun avulla. Kun käyttäjä omistaa NFC-ominaisuuden sisältävän matkapuhelimen, hän voi tilata pankista MasterCard PayPass -palvelun. Käyttäjä lataa kortin maksutiedot matkapuhelimeensa ja aktivoi siihen maksusovelluksen. Tämän jälkeen matkapuhelin on käyttövalmis. Kun käyttäjä menee esimerkiksi kauppaan, hän tarkistaa onko kassalla MasterCard PayPass -lukulaitetta. Jos maksaminen onnistuu, käyttäjä avaa maksusovelluksen ja vie matkapuhelimensa lukulaitteen luokse. Maksupääte ilmoittaa maksun onnistumisesta valo- ja äänimerkillä. Kun ostokset maksavat korkeintaan 25 dollaria, ei maksettaessa tarvita tunnistautumista. (MasterCard 2012.)

Ajantasainen lista tällä hetkellä markkinoilla olevista NFC-matkapuhelimista löytyy esimerkiksi matkapuhelinvalmistajien tai NFC Worldin kotisivuilta.

NFC-ominaisuus matkapuhelimeen SIM-kortilla

Tätä mahdollisuutta ei ole vielä massatuotannossa, mutta useat eri yritykset ovat pyrkineet tuomaan ratkaisun markkinoille. Näin jokainen matkapuhelin teoriassa voisi tulevaisuudessa saada NFC-ominaisuuden. (Ray 2011.)

NFC-ominaisuuden lisääminen SIM-kortille on ollut haasteellista. Jo vuonna 2006 italialainen Telecom Italia julkisti oman tuotteensa prototyypin, mutta ei koskaan onnistunut esittelemään toimivaa tuotetta. Vuoden 2011 lopussa ranskalainen Inside Secure esitteli oman NFC-ominaisuuden sisältävän SIM-korttiratkaisunsa. Inside Securen SIM-kortissa on luovuttu kokonaan passiivisesta NFC-ratkaisusta, joten toimiakseen SIM:llä sijaitseva NFC-tunniste tarvitsee virtaa puhelimelta. Virran kulutus ei kuitenkaan ole suurta ja puhelimet, joihin NFC-SIM-kortteja tarvitaan, ovat joka tapauksessa peruspuhelimia, joiden akun kesto on aivan omaa luokkaansa esimerkiksi tämän päivän älypuhelimiin verrattuna. Inside Securen NFC-antenni on kooltaan 5 x 10 millimetriä, joten se

voidaan sijoittaa standardikokoiselle SIM-kortille. Näin käytettävistä puhelimista rajautuu pois versiot, jotka käyttävät micro-SIM-korttia. Yritys myöntää myös, ettei sen NFC-SIM-kortti tule toimimaan kaikissa puhelinmalleissa täydellisesti. Sen pitäisi kuitenkin toimia pääsääntöisesti ongelmitta. Toteutuessaan NFC-SIM-kortti laajentaa NFC-teknologian markkinoita huomattavasti ja edesauttaa tekniikan nopeampaa leviämistä. Tämä asettaa NFC-SIM-kortin teleoperaattorien valvontaan ja päätösvaltaan siitä, mitä maksutekniikoita NFC-turvaelementille (joka myös sijaitsee SIM-kortilla) sisällytetään. (Ray 2011.)

NFC-ominaisuus matkapuhelimeen tarralla

Tällä hetkellä NFC-siru löytyy integroituna vain harvoista matkapuhelimista. Tämä ei kuitenkaan ole este NFC:n hyödyntämiselle, koska matkapuhelimiin on mahdollista lisätä NFC-toiminto takakanteen liimattavan NFC-sirun sisältävän tarran avulla (kuva 8). Tarroja voidaan käyttää esimerkiksi pienten maksujen maksamisessa tai lentokentän lähtöselvityksessä. (Bank of Montreal 2012.)

Kuva 8. NFC-tarra liimattuna matkapuhelimen takakanteen. (Kuva: Julien Houbrechts.)

Esimerkiksi Kanadassa MasterCardilta on saatavilla MasterCard Mobile PayPass -tarra, joka on mahdollista tilata ilmaiseksi soittamalla. Tarra lähetetään tilaajalle postissa, jonka jälkeen se on vielä aktivoitava käyttöön soittamalla pankkiin. Kun tarra on aktivoitu ja liimattu puhelimen takakanteen, sillä voidaan maksaa esimerkiksi kaupassa, kahvilassa tai automaatilla, jossa on PayPass-maksamista tukeva maksupääte. Maksusta lähetetään aina ilmoitus myös käyt-

täjän sähköpostiin. Ostokset voivat maksaa kerralla enintään 50 dollaria. (Bank of Montreal 2012.) Tarralla maksaminen muistuttaa suurelta osin NFC-älykortilla maksamista. Puhelimeen ei tarvitse asentaa maksusovellusta, sillä käyttäjän tarvitsee vain viedä tarra lähelle maksupäätettä, joka lukee tarraan sisällytetyt maksutiedot.

3.3.2 NFC-ominaisuus älykortissa

NFC-teknologiaa voidaan hyödyntää matkapuhelinten lisäksi myös niin sanotuissa kontaktittomissa älykorteissa (Kuva 9). Kortin muistiin voidaan tallentaa erilaisia lippuja, kuponkeja tai leimakortteja, sekä jotakin arvoa tai palvelurahaa. (Suikkanen 2011b, 3.)

Kuva 9. Lontoon julkisen liikenteen kontaktiton maksukortti. (Kuva: Karl Baron.)

NFC-matkapuhelinten lisäksi myös älykorteilla voidaan maksaa Suomessa alle 20 euroa maksavia ostoksia. Tällöin ei tarvita tunnuslukua, vaan maksamiseen riittää kortin näyttäminen lukijalaitteen läheisyydessä. Jos ostosten arvo on pankin määrittelemää maksurajaa suurempi, käytetään turvallisuuden varmistamiseen laskureita, jotka vaativat sirukortin ja tunnusluvun avulla suoritettavan online-tarkistuksen. (Luottokunta 2012c.)

3.3.3 NFC-tunnisteet

NFC-tunnisteita on saatavilla useissa eri muodoissa. Tunnisteet voivat olla esimerkiksi sisä- ja ulkotilojen tarroja, kortteja tai avaimenperiä. Niihin on mahdollista kirjoittaa tietosisältöä standardin mukaisessa NDEF-formaatissa, jolloin

tieto on mahdollista lukea kaikilla NFC-matkapuhelimilla. Tunnisteiden ohjelmointi ja tiedon kirjoitussuojaus on mahdollista tehdä itse siihen tarkoitetuilla laitteilla ja ohjelmilla. Tietosisällön lisäksi myös tulostus voi olla jokaisella tunnisteella yksilöllistä. Tunnisteita on saatavilla asiakaskohtaisella värillisellä ulkoasulla, johon voidaan lisätä esimerkiksi yrityksen oma logo. (ToP Tunniste Oy 2012a.)

Jos NFC-tunnisteita viedään esimerkiksi turistinähtävyyden luo, voi matkailija saada lisätietoa kohteesta esimerkiksi matkapuhelimeen tai tietokoneelle. Kun tunnistetta hipaisee, voi se esimerkiksi johdattaa käyttäjän halutulle internetsivulle. Sama periaate toimii myös monissa muissa käyttökohteissa, kuten esimerkiksi älyjulisteeseen kiinnitetyssä tunnisteessa (kuva 10), jolla voidaan ohjata käyttäjä avaamaan toimintoja, kuten menemään esimerkiksi verkkokauppaan hakemaan lisätietoa tai ostamaan konsertti- tai muita pääsylippuja. (NFC-työryhmä 2011, 8.)

Kuva 10. NFC-tunniste älyjulisteessa. (Kuva: Tupalo.com.)

Ravintolan pöydässä oleva tunniste voi ohjata asiakkaan tilaamaan annoksensa tunnisteen avaaman sovelluksen välityksellä (kuva 11) ja kaupassa asiakas voi nopeuttaa kassatapahtumaa kanta-asiakas- tai maksusovelluksissa NFC-tunnisteella, joka voi sijaita esimerkiksi kukkarossa. (NFC-työryhmä 2011, 8.)

Kuva 11. Esimerkiksi ravintolassa on mahdollista tehdä tilaus NFC-tunnistetta hyödyntäen. (Kuva: Pierre Metivier.)

Teollisuusjärjestö NFC Forumin mukaan NFC-tunnisteet voidaan jakaa eri tunnistetyyppeihin seuraavasti (Sunsero 2012).

NFC Forum Type 1

Tunnisteessa on käytettävää muistia 96 tavua, jota voidaan kasvattaa 2 kilotavuun. Kommunikointinopeus on 106 kbit/s. Tunnisteelle on mahdollista kirjoittaa ja uudelleenkirjoittaa tietoa. Tunniste on mahdollista asettaa myös kirjoitussuojatuksi. Tunniste perustuu ISO14443-A –standardiin ja siruna on Topaz™. (Sunsero 2012.)

NFC Forum Type 2

Tunnisteessa on käytettävää muistia 48 tavua, jota voidaan kasvattaa 2 kilotavuun. Kommunikointinopeus on 106 kbit/s. Tunnisteelle on mahdollista kirjoittaa ja uudelleenkirjoittaa tietoa. Tunniste on mahdollista asettaa myös kirjoitussuojatuksi. Tunnisteet voivat olla esimerkiksi ulkotilan nfc-tunnisteita, sisätilan NFC-tarroja, NFC-kortteja sekä avaimenperätunnisteita. Tunniste perustuu ISO14443-A standardiin. Siruvaihtoehdot ovat Mifare Ultralight (NXP) - 48 tavua ja Mifare Ultralight C (NXP) - 144 tavua. (Sunsero 2012.)

NFC Forum Type 3

Tunniste perustuu japanilaiseen teollisuusstandardiin JIS X 6319-4 (Japanese Industrial Standard). Siruna FeliCa (Sony). Tunnisteisiin esi-asetetaan valmis-

tuksen yhteydessä tietty lukuoikeus (luku ja uudelleenkirjoitus, tai ainoastaan lukuoikeus). Teoreettisesti muisti on kutakin sovellusta kohti maksimissaan 1 megatavun, mutta muistin määrä vaihtelee. Kommunikointinopeus voi olla 212 kbit/s tai 424 kbit/s. (Sunsero 2012.)

NFC Forum Type 4

Tunnisteessa käytettävissä olevan muistin määrä vaihtelee. Muistia voi olla kutakin sovellusta kohti jopa 32 kilotavua. Kommunikointinopeus on to 424 kbit/s. Tunnisteisiin esi-asetetaan valmistuksen yhteydessä tietty lukuoikeus (luku ja uudelleenkirjoitus, tai ainoastaan lukuoikeus). Tunniste perustuu ISO 14443-A ja ISO 14443-B -standardeihin. Siruna on Mifare DESfire (NXP). (Sunsero 2012.)

Mifare Standard 1k

Tunniste ei ole NFC Forumin hyväksymä tunnistetyyppi sen suojausalgoritmin julkistamiseen liittyvien rajoitteiden vuoksi. Tunnisteessa on käytettävää muistia noin 768 tavua ja se jakaantuu 16 sektoriin. Kommunikointinopeus on 106 kbit/s. Tunnisteelle voidaan kirjoittaa ja uudelleenkirjoittaa tietoa. Käyttäjä voi myös asettaa tunnisteeseen kirjoitus- ja lukusuojauksen sektorikohtaisilla avaimilla. Tunniste on ollut saatavilla kaupallisesti jo pitkän aikaa. Sitä on käytetty esimerkiksi maksu- ja lippusovelluksien lisäksi RFID- ja NFC-ratkaisuissa, joissa NFC Type 2 -kategoriaan kuuluvan Mifare Ultralight -tunnisteen muisti ei riitä. Tunnistetyyppi on luotettava, kustannustehokas ja se soveltuu monenlaisiin käyttötarkoituksiin. Mahdollisuus sektorikohtaisten kirjoitus- ja lukuavainten käyttöön tuo joissakin käyttökohteissa etuja, jotka päihittävät NFC Forumin nimeämät tunnistetyypit. Tunniste perustuu ISO 14443-A -standardiin. Siruna on Mifare Standard 1k (NXP). (Sunsero 2012.)

3.3.4 Lukulaitteet

NFC-lukija voi sijaita matkapuhelimessa tai olla erillinen laite. Olemassa on lukulaitteita, jotka pystyvät sekä lukemaan että kirjoittamaan tunnisteita. Näiden lisäksi on laitteita, joilla onnistuu ainoastaan lukeminen. Lukija voidaan laitemallista riippuen liittää tai integroida osaksi muuta maksuratkaisua. (Top Tunniste Oy 2012b.) Maksupäätteiden lisäksi markkinoilla on olemassa esimerkiksi suoraan tietokoneeseen USB-liitännällä liitettäviä lukijoita, sekä erillisinä moduuleina laitteisiin liitettäviä lukijoita. Moduulityyppisiä lukijoita käytetään yleensä sulautetuissa ratkaisuissa, kuten esimerkiksi nettikioskeilla tai juoma-automaateissa. Suoraan tietokoneeseen USB-liitännällä kytkettäviä lukulaitteita on myynnissä myös yksityiskäyttöön ja laitteisiin on yleensä tarjolla myös SDK-paketteja (ohjelmistokehityspaketteja).

Lähimaksupäätteet

Luottokunta kannustaa ihmisiä lähimaksua tukevien maksupäätteiden ja maksukorttien hankintaan. Kaupan liiton asiamies Matti Räisäsen mukaan lähimaksamisesta tulee arkipäivää, kun kauppojen maksupäätteitä ja maksukorttikantaa uudistettaessa niistä löytyy yhä useammin myös lähimaksuominaisuus. Luottokunnan myyntijohtaja Jukka Koivu ennustaa lähimaksukorttien yleistyvän Suomessa viimeistään vuoden 2013 aikana. (Luottokunta 2011a, 1 - 2.) Jo nyt lähimaksupäätteitä on otettu käyttöön Suomessa useita tuhansia ja niiden sertifiointi Visan ja MasterCardin vaatimuksien mukaiseksi on aloitettu vuonna 2012. Arvion mukaan Suomen maksupäätteistä noin puolet tukee lähimaksamista vuonna 2015. (Luottokunta 2011b.)

Lähimaksuominaisuudella varustettuja maksupäätteitä on ollut saatavilla esimerkiksi luottokunnalta vuoden 2012 huhtikuusta alkaen. Valikoimista löytyy sekä kassaympäristöön asennettavat, että itsenäisesti käytettävät maksupäätemallit. Kuukausimaksuun sisältyy kaikki tarpeellinen: maksupääte, ohjelmistot, varmennuspalvelut ja turvallisen aineiston siirto, verkkopalvelun kautta onnistuva tapahtuman seuranta, automaattiset päivitykset sekä käyttötuki arkisin ja viikonloppuisin. (Luottokunta 2012d.)

Kuvassa 12 havainnollistetaan NFC-matkapuhelimella suoritettavaa maksutapahtumaa, jossa matkapuhelin viedään maksupäätteen lähelle.

Kuva 12. NFC-matkapuhelin maksutilanteessa. (Kuva: Pierre Metivier.)

Lähimaksupäätteiden lisäksi rahan siirtäminen onnistuu myös henkilöltä toiselle henkilölle (P2P) kahden matkapuhelimen välillä (Kapanen 2010, 4). Rahansiirrossa tai pienessä kaupankäynnissä rahan lähettäjän puhelin toimii tunnisteena ja vastaanottajan puhelin lukijana. Esimerkiksi PayPal tarjoaa rahansiirtoa PayPal-tililtä toiselle NFC:n avulla. Molemmilla osapuolilla täytyy olla asennettuna PayPal-maksusovellus. Maksusovelluksessa valitaan rahansiirtotoiminto (rahan pyytäminen tai lähettäminen) ja siirrettävä summa, jonka jälkeen hipaistaan puhelimia yhteen ja vastapuoli hyväksyy siirron. (Chambers 2011.)

Muut lukulaitteet

Lukulaitteiden kirjo on laaja, niitä löytyy paljon erilaisia maksamisen lisäksi myös moniin muihin eri käyttötarkoituksiin. Tyypillisiä käyttökohteita voivat olla esimerkiksi kulunvalvonta, kanta-asiakkuusohjelmat, julkinen liikenne, elektroniset terveydenhuollon järjestelmät, sekä julkinen asiointi. Markkinoilla on myös edullisia ja hyvin yksinkertaisiakin lukulaiteratkaisuja, jotka soveltuvat myös yksityiskäyttöön. Yksi tällainen on esimerkiksi ACR122U-lukulaite. (Advanced Card System Ltd 2012.)

Myös Tikitag (kuva 13) on tietokoneen USB-porttiin kiinnitettävä RFID-lukija, jolla voidaan siirtää tunnisteiden sisältämiä tietoja tietokoneelle (Cangeloso 2008).

Kuva 13. Tietokoneeseen liitettävä lukulaite (Kuva: Josh DiMauro.)

3.4 NFC-maksamisen nykytilanne

EMV-standardin mukaiset älykortit ovat korvanneet magneettijuovalla varustetut kortit viimeisen vuosikymmenen aikana. Sirukortti on magneettikorttia turvallisempi ja mahdollistaa kortille huomattavasti suuremman tietomäärän tallentamisen. Kortit edellyttivät aikaisemmin kontaktin ottamista kortinlukulaitteeseen, mutta NFC-tekniikan myötä ovat myös kontaktittomat älykortit tulleet mahdollisiksi. (NFC-työryhmä 2010, 5.)

NFC-tekniikan sovellutuksien ensimmäiset standardit hyväksyttiin vuonna 2003. Seuraavana vuonna Nokia, Sony ja Philips perustivat yhdessä voittoa tavoittelemattoman NFC Forumin edistämään NFC-laitteiden käyttöä ja kehitystä. Tällä hetkellä NFC Forumiin on liittynyt jo yli 140 jäsenorganisaatiota. (NFC-työryhmä 2010, 5.)

Lähiasiointi kontaktitonta tekniikkaa hyödyntäen ei ole Euroopassa vielä yhtä laajalti käytössä kuin Aasiassa ja erityisesti Japanissa, jossa niin sanottua mobiili koodausta (mobile tagging) käytetään runsaasti mobiilimarkkinoinnissa. Mobiili koodauksessa luetaan kaksiulotteisia tunnisteita käyttämällä lukulaitteena matkapuhelinta. Nämä tunnisteet voivat antaa esimerkiksi lisätietoa tuotteesta, johon tunniste on kiinnitetty, tai tunniste voi ohjata käyttäjän halutulle verkkosivulle. Tällä hetkellä yksi suurimmista toiminnassa olevista NFC-maksamiseen liittyvistä hankkeista on Japanilaisella NTT Docomo -mobiilioperaattorilla, jonka yli kymmenen miljoonan asiakkaan matkapuhelimiin on asennettu luottokorttiominaisuuden sisältävä palvelu nimeltä Osaifu-Keitai. Palvelun avulla asiakkaan on myös mahdollista ostaa matkalippu tai käyttää matkapuhelinta henkilö- tai kulkukorttina. Palvelun käyttäminen on mahdollista jo noin 420 000 kortinlukupisteessä. Palveluiden laajan markkinoille tuonnin Japanissa on mahdollistanut NTT Docomon määräävä markkina-asema. (NFC-työryhmä 2010, 5 - 9.)

Mobiilimaksamista on kokeiltu Euroopassa jo yli 20 maassa. Toteutus on kuitenkin edelleen pysynyt pitkään kokeiluasteella. NFC-teknologiaa hyödynnetään tällä hetkellä lähinnä maksettaessa matkalippuja. Myös Suomessa on käytössä NFC:tä hyödyntäviä järjestelmiä, joista kaikkein suurin on HSL:n (Helsingin Seudun Liikenteen) matkakorttijärjestelmä. Järjestelmät ovat toimittajakohtaisia, koska valtakunnallista lippustandardia ei vielä tällä hetkellä ole olemassa. (NFC-työryhmä 2011, 4 - 7.)

Kontaktiton lähimaksaminen on suosituinta hinnaltaan edullisten ostosten maksamisessa. Maksutapa onkin kehittynyt parhaiten juuri maissa, joissa käteisellä maksaminen on runsasta. Vähäarvoiset käteismaksut ovat aikaa vieviä ja kysyntä helpommalle ratkaisulle onkin ollut näissä maissa muita maita suurempaa. Maissa, joissa käytetään runsaasti luottokortteja (esimerkiksi pohjoismaat kuten Suomi), kehitys on ollut muita hitaampaa. Myös markkinoiden pienuus on osaltaan voinut vaikuttaa lähimaksamisen hitaaseen kehitykseen. (NFC-työryhmä 2010, 6.)

NFC:n kehitystä ja lähimaksamisen yleistymistä ovat hidastaneet suurelta osin myös tekniset rajoitukset. NFC-ominaisuus löytyy tällä hetkellä vain harvoista matkapuhelimista. Maailman ensimmäinen matkapuhelin, joka sisälsi täysin integroidun NFC-lukijalaitteen, oli Nokia 6131 NFC, joka tuli markkinoille vuonna 2006. Lähiaikoina on odotettavissa, että markkinoille tulee myyntiin nykyistä huomattavasi suurempi määrä NFC-ominaisuuden sisältäviä matkapuhelimia. Japanissa on myynnissä satoja eri puhelinmalleja, jotka käyttävät Felica-kosketusteknologiaa. Kyseessä on vastaavanlainen teknologia kuin NFC. (NFC-työryhmä 2010, 6.)

ABI Research-tutkimusyhtiön mukaan vuosi 2011 tuotti mobiilimaksamisen kannalta pettymyksen, koska NFC-matkapuhelimet eivät yleistynetkään niin nopeasti kuin oli odotettavissa. Mobiilimaksamisen yleistymisen hitautta selitetään sillä, että operaattorien oli ryhdyttävä loppuvuonna miettimään uusiksi bisnesmallejaan. Monet operaattorit erehtyivät luulemaan luottokorttiyhtiöiden maksavan niille korttien sisällyttämisestä matkapuhelinliittymiin, mutta näin ei lopulta tapahtunut. Teknologian kehitys kuitenkin meni eteenpäin, kun esimerkiksi Google lanseerasi kehittämänsä Wallet-palvelun. Operaattorit ryhtyivät palvelun myötä kehittämään monissa maissa yhteistä palvelua mobiilimaksuille. Wallet-palvelun odotetaan kasvavan hitiksi vuoden 2012 loppuun mennessä. AT&T:n, T-Mobilen ja Verizon Wirelessin lanseeraama Isis-mobiilimaksujärjestelmä odotetaan tulevan vuoden 2012 kesään mennessä käyttöön Austinissa, Teksasissa ja Salt Lake Cityssä. Järjestelmän odotetaan olevan käytössä koko Yhdysvaltojen laajuisena vuonna 2013 tai 2014. (Kolehmainen 2012.)

Abi Researchin johtaja John Devlin on korostanut, että tällä hetkellä kilpailua käydään siitä, kuka ehtii markkinoille ensimmäisenä. Operaattorit pelkäävät asemansa menettämistä, jos Googlen Wallet-palvelu ehtii vakiinnuttaa asemansa ennen niitä. Jotkut analyytikot ovat varmoja siitä, että myös Apple tulee lanseeraamaan oman maksujärjestelmänsä ja tuo osaltaan markkinoille vielä lisää kilpailua. Apple todennäköisesti lanseeraakin oman mobiililompakkonsa vuoden 2012 aikana. Teknologian menestymisen kannalta on erityisen tärkeää, että eri tarjoajien mobiilimaksut ovat keskenään yhteensopivia. Vielä tällä hetkellä val-

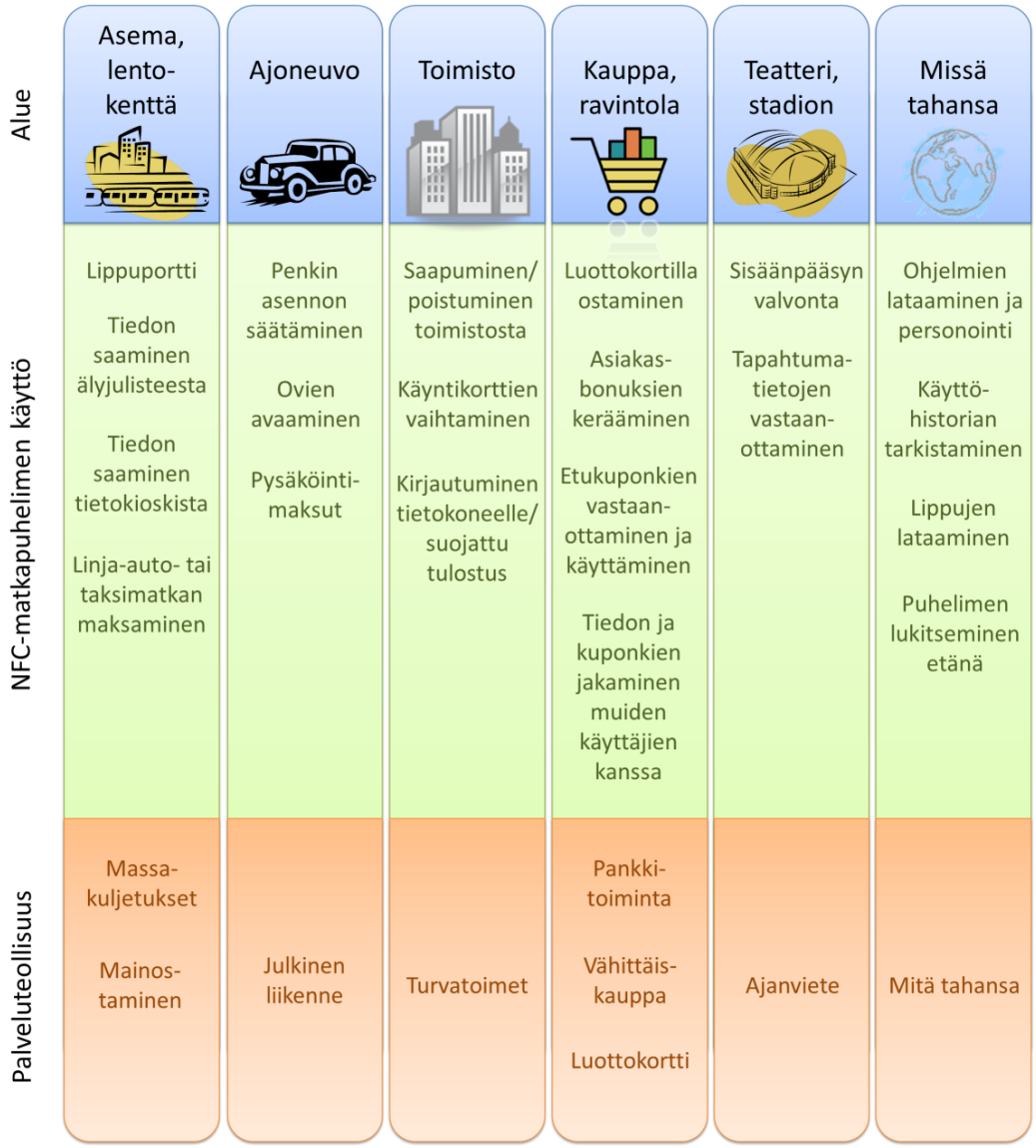
mistajat pitävät tiukasti kiinni omista ratkaisuistaan, mutta yhteisratkaisun uskotaan vielä lopulta löytyvän. (Kolehmainen 2012.)

NFC-matkapuhelinten määrän on arvioitu kasvavan vuoden 2012 aikana tutkimusyhtiön mukaan 24 miljoonasta jopa 80 miljoonaan. Läpimurtoa mobiilimaksamisessa ei kuitenkaan vielä tänäkään vuonna ole nähtävissä, vaan massamarkkinat uskotaan saavutettavan vasta vuoden 2016 tienoilla, jolloin matkapuhelinten laitemäärän uskotaan ylittävän 552 miljoonaa kappaletta. (Kolehmainen 2012.)

3.5 NFC:n mahdollisuudet erilaisissa käyttöympäristöissä

NFC-ominaisuuden avulla toteutettavia käyttökohteita voidaan usein kuvata sähköiseksi lähiasioinniksi, jossa asiointi- tai palvelutapahtumassa mukana olevat henkilöt ovat samassa paikassa fyysisesti läsnä. Palvelutapahtuma saa sähköisen elementin, kun siihen liitetään NFC. Tämä nopeuttaa asiointia ja tekee siitä helpompaa. Myös inhimillisten erehdysten määrä häviää erityisesti palveluntarjoajan puolelta. (NFC-työryhmä 2011, 3.) NFC:tä voidaan pitää kuluttajan näkökulmasta fyysisenä käyttöliittymänä palveluiden aktivoimiseen, joka tapahtuu kosketuksen avulla. Useissa tapauksissa käyttäminen ei vaadi laincaan matkapuhelimen näppäimistön käyttämistä. (Seppä 2011, 18.) Lähiasiointi NFC:n avulla vastaa suurelta osin kasvokkain perinteisillä menetelmillä tapahtuvaa asiointia. Esimerkiksi kysymys henkilöllisyydestä ei tämän kaltaisessa asioinnissa ole samalla tavalla tärkeää kuin etäasioinnissa, joka tapahtuu tietoverkkojen ylitse. (NFC-työryhmä 2011, 3.)

NFC-teknologia helpottaa monia toimintoja jokapäiväisessä elämässä (kuva 14). Kaikkein yksinkertaisimmin NFC:n merkitystä kuluttajille voidaan kuvata siten, että standardi mahdollistaa kaikkien kukkarossa olevien korttien (esimerkiksi pankkikortit, luottokortit, henkilöllisyystodistukset, asiakaskortit) ja lippujen (matkaliput, teatteriliput, maksukuitit ja vastaavat) löytymisen matkapuhelimesta. (Seppä 2011, 18.)



Kuva 14. Esimerkki NFC:n vaikuttamisesta jokapäiväiseen elämään (NFC Forum 2012).

Tällä hetkellä yksi laajimmin käytössä olevista NFC:n sovelluksista on niin sanottu biopassi, joita on käytössä Suomessa useita satoja tuhansia ja muualla maailmassa jopa kymmeniä miljoonia. Esimerkiksi Helsingin Seudun liikenteen matkakortit perustuvat samoihin standardeihin ja myös muissa palveluissa niiden henkilökohtaisia versioita hyödynnetään henkilötunnisteina. (NFC-työryhmä 2010, 8.) Biopassien lisäksi kontaktitonta lähiasiointia hyödynnetään eniten myös ostettaessa matkalippuja tai maksettaessa muita pieniä ostoksia (NFC-työryhmä 2010, 15). Matkapuhelinta voidaan käyttää myös tärkeiden avainten toimintaan. Tällaisia ovat esimerkiksi auton, kodin ja työpaikan ovien avaami-

nen. (Seppä 2011, 18.) Alla on esitetty esimerkkejä NFC:n käyttömahdollisuuksista erilaisissa käyttöympäristöissä.

3.5.1 Kaupassa

Tulevaisuudessa asiakkaat voivat saada kaupassa matkapuhelimeensa ostosten tuotetiedot viemällä NFC-matkapuhelimen tuotteeseen kiinnitetyn tunnisteen luokse. Myös esimerkiksi iäkkäät ja erityisruokavalioita noudattavat henkilöt voivat hyötyä saadessaan yksityiskohtaisempaa tietoa harkitsemansa ostoksen sisällöstä. Tunnisteen avulla voidaan saada selville esimerkiksi tuotteen alkuperä (valmistuspaikka, elintarvikkeiden tuottajatila) sekä sen tuottama hiilidioksidijalanjälki. Kun asiakas voi nähdä tunnisteen avulla saman tuotteen hinnan muissakin kaupoissa, helpottuu myös tuotteiden hintavertailu. Tulevaisuudessa kuluttaja voi myös maksaa ostoksensa kaupassa ilman kassahenkilökuntaa, kun ostoksista kerätään lista koskettamalla tuotteiden tunnisteita matkapuhelimella. Ostoksia on mahdollista myös vertailla matkapuhelimessa olevaan ostoslistaan. (Seppä 2011, 18.)

NFC-lähitunnistustekniikkaa on ilmoittanut ottavansa käyttöön tällä hetkellä esimerkiksi Ruotsalainen päivittäistavaraketju ICA, joka ottaa käyttöönsä digitaalisen leimakortin. Laitteet on otettu käyttöön ensin Tukholmassa alueella, jossa sijaitsee paljon IT-yrityksiä ja Kuninkaallinen teknillinen korkeakoulu. ICA:n kauppoihin on asennettu NFC-yhteensopivat laitteet, jotka lukevat digitaalisia leimoja, mutta eivät vielä kuitenkaan tue NFC-maksamista. Leimoja voidaan käyttää ICA To Go -konseptiliikkeissä. (Vänskä 2012.)

NFC-tuki on integroituna vielä nykyaikana vain hyvin harvoissa matkapuhelimissa, joten asiakkaille jaetaan ilmaisia NFC-sirutarroja Ican-kaupoissa. Asiakas pystyy synkronoimaan NFC-sirutarran puhelimeen asennetun Formica-sovelluksen kanssa. Leimattaessa puhelinta pidetään lukulaitteen päällä. Leimoja saa aluksi vain lounaslaatikoista, mutta kaupan tarkoituksena on laajentaa tuotteita tulevaisuudessa myös esimerkiksi kahvimukeihin. Ica To Go:n markkinointijohtaja Helene Robertsonin mukaan ei voida vielä sanoa varmaksi, milloin

NFC:llä maksaminen voi oikeasti tulla käyttöön ICA:n kaupoissa. Maksutavan uskotaan kuitenkin tulevan käyttöön viiden vuoden sisällä, sillä Robertsonin mukaan NFC tarjoaa täydellisen ratkaisun pikkuostoksien maksamiseen. (Vänskä 2012.)

Suomessa tällä hetkellä K-Plussa on ilmoittanut ottavansa käyttöön etäluettavat K-Plussa-käteiskortit. K-Plus Oy:n toimitusjohtaja Niina Ryynäsen mukaan etäluku helpottaa asiointia kassalla. Korttia ei tarvitse enää vetää läpi lukulaitteesta, vaan riittää että asiakas käyttää korttia lukulaitteen läheisyydessä. Laite lukee kortin asiakastunnisteen, jolloin se rekisteröi kertyvät K-Plussa-pisteet sekä muut etuudet. Etäluettava K-Plussa-kortti on Suomen vähittäiskaupassa kaikkein suurin etälukutekniikalla toimiva sovellus. Mobiiliratkaisujen ja etäluettavan maksamisen kehittymistä seurataan aktiivisesti yhteistyökumppaneiden kanssa. (Kesko 2012.)

Myös OP-Pohjola on ilmoittanut ottavansa lähiluettavat maksukortit käyttöönsä. Mikäli ostokset maksavat alle 25 euroa, ei maksajan tarvitse antaa korttinsa PIN-koodia. Maksamiseen riittää, että maksaja pitää korttia maksupäätteen edessä muutaman sekunnin ajan. Maksupääte ilmoittaa maksun onnistumisesta merkkiäänellä ja -valolla. Suuremmat maksut on edelleen suoritettava perinteiseen tapaan laittamalla kortti lukijaan ja antamalla PIN-koodi. (OP-Pohjola-ryhmä 2012.)

NFC-kortit tukevat MasterCardin PayPass- ja Visa PayWave -tekniikoita (Pitkänen 2012). Tavoitteena on, että NFC-ominaisuus tulee kaikkiin uusiin ja uusittaviin OP-Visa Debit -kortteihin vuoden 2012 syksystä lähtien. Ominaisuus lisätään muihin kortteihin myöhemmin. Kortit toimivat Suomessa ja ulkomailla kaupoissa, joissa on lähimaksamista tukevat maksupäätteet. Nämä tunnistaa lähimaksamislogosta. (OP-Pohjola-ryhmä 2012.) Luottokunta on tuonut sopivat maksupäätteet saataville jo vuonna 2011. NFC-maksupäätteitä on ilmoittanut tuovansa markkinoille tulevaisuudessa myös Elisa. (Pitkänen 2012.)

3.5.2 Ravintolassa

NFC:n mahdollisuuksia on testattu esimerkiksi Oulussa sijaitsevassa Ravintola Pannussa ja Oluthuone Leskisessä vuonna 2007. Halutessaan kokeilla NFC:llä maksamista, Ravintola Pannun asiakas pystyi asentamaan NFC-matkapuhelimeensa ohjelmiston. Tämän jälkeen ravintolassa oli mahdollista tehdä tilauksia koskettamalla matkapuhelimella ensin pöydässä olevaa NFC-tunnistetta ja tämän jälkeen koskettamalla menusta haluamiaan tuotteita. Tilaus lähetettiin TeliaSoneran välitysjärjestelmään, joka toimitti tilauksen ravintolan maksujärjestelmään ja keittiöön. Myös elektroniset lounaskupongit oli mahdollista lunastaa NFC-tilausjärjestelmässä. Matkapuhelimeen oli mahdollista ladata kuponkeja, jotka poistettiin aina tilauksen jälkeen. Asiakkaat saivat halutessaan lisätietoa ravintolan pöydille sijoitetuista älyjulisteista. Ravintolan omistajat saivat idean kokeilla lounaiden tilaamisessa NFC:tä, koska halusivat kiireisiin lounasaikoihin lisää suoritustehoa ja tuottavuutta. Ravintolassa haluttiin myös päästä eroon paperisista kupongeista. (City of Oulu -project 2008, 11.)

Oluthuone Leskisessä olleen projektin aikana asiakkaiden oli mahdollista ”kirjautua sisään” oluthuoneelle koskettamalla NFC-matkapuhelimella ulko-oven lähellä olevaa NFC-tunnistetta, jolloin asiakas merkittiin Leskisen kanta-asiakasjärjestelmässä ”sisään kirjautuneeksi”. Järjestelmään kirjautuneiden oli mahdollista saada SMS-pohjaista markkinointitietoa tai erikoistarjouksia koskettamalla markkinointitunnistetta matkapuhelimellaan. Tiedot oluista ja muista tarjolla olevista tuotteista oli saatavilla julisteissa ja pöydillä sijaitsevissa tunnisteissa. (City of Oulu -project 2008, 11.)

Lähimaksaminen yleistyy tällä hetkellä nopeasti myös pikaruokaravintoloissa ainakin Iso-Britanniassa, jossa arvioidaan olevan tällä hetkellä yli 20 miljoonaa lähimaksukorttia. Maksaminen onnistuu yli 60 000 myyntipisteessä ja maksutapa on yleistynyt Lontoon olympialaisten alla nopeasti useissa paikoissa. Esimerkiksi hampurilaisravintola McDonalds on ryhtynyt ottamaan vastaan lähimaksuja kaikissa ketjun ravintoloissa ympäri Iso-Britanniaa. Asiakaspalvelun lisänopeus tuo pikaruokapaikoille selvän kilpailuedun. Vaikka Iso-Britanniassa lähimaksun yläraja on 15 puntaa, soveltuu maksuratkaisu hampurilaisravintolal-

le erittäin hyvin, koska McDonaldsin yksittäisistä ostoksista suurin osa alittaa tämän summan. Lähimaksaminen nopeuttaa kassojen läpimenoaikoja sekä vähentää ravintolalle koituvia kuluja käteismaksujen vähentyessä. Lähimaksaminen on toteutettu Ingenico-lähimaksupäätteillä. (Luottokunta 2012e, 1.)

Ruotsalaisen Computer Sweden -teknologiasivuston järjestämässä testissä NFC:llä maksaminen onnistui helposti ja vei aikaa vain noin kahden sekunnin verran. Tekniikan käyttäminen pienten kertamaksujen maksamiseen voisi vähentää ruuhkaa paikoissa, joissa on kiire palvella paljon asiakkaita. Ruuhkaiset tiskit saavat kärsimättömät asiakkaat vaihtamaan ravintolaa, joka vaikuttaa yrityksen toimintatehoon ja toiminnasta saatavaan tuottoon. Perinteisten korttien käytöstä syntyy myös käsittelykuluja, jotka ovat suurempia kuin uusissa maksupäätteissä. (Vänskä 2011.)

3.5.3 Teatterissa

Tulevaisuudessa on hyvin mahdollista, että NFC:tä tullaan hyödyntämään myös teattereissa. Vuonna 2007 Oulun kaupungin teatteri oli ensimmäinen kulttuurilaitos maailmassa, joka pilotoi NFC-teknologiaa kaikessa asiakaspalvelussa rikastaakseen kävijöiden teatterikokemusta. Pilottiprojekti kattoi yhdeksän teatteriesitystä ja palvelukokonaisuutta kokonaisen teatteri-illan aikana ja kokeiluun valittiin etukäteen NFC:tä testaavia käyttäjäryhmiä. Testiryhmät koostuivat eri yritysten henkilöstöstä ja eri yhteisöjen jäsenistä. (City of Oulu -project 2008, 10.)

Pilottiin osallistuneet henkilöt vastaanottivat teatteriliput langattomasti TeliaSoneran taustajärjestelmästä tai suoraan teatterin myyntipisteestä NFC:tä hyödyntäviin matkapuhelimiinsa. Laskutustiedot tallennettiin taustajärjestelmään ja varsinainen laskutus suoritettiin vasta jälkeen päin. Pilottikäyttäjät pystyivät tilaamaan väliaikapalveluita ennakkoon käyttäen NFC-matkapuhelinta, teatterisovellusta ja menukorttia. Teatterin ohjelma sisällytettiin sisäänpääsymaksuun ja sen sai käyttöönsä koskettamalla tunnistetta matkapuhelimella. (City of Oulu -project 2008, 10.)

Teatterin ravintolassa asiakkaat saivat älyjulisteista informaatiota esimerkiksi paikallisista uutisista. Myös videoita oli mahdollista ladata esimerkiksi nähdäkseen ohjaajan ajatuksia esityksestä. Videot räätälöitiin mobiililaitteiden pienille ruuduille sopiviksi Oulun seudun ammattikorkeakoulun NeoArena-projektin toimesta. Projektin suunnittelivat Oulun teatteri ja ravintolapalveluita tarjoava Kanresta. Teknisistä ratkaisuista vastasivat TeliaSonera ja MSG Software. (City of Oulu -project 2008, 10.)

3.5.4 Koulussa

Vuonna 2008 Oulussa toteutettiin projekti, jossa kokeiltiin NFC:tä oppilaiden oppitunneille osallistumisen valvontaan. Järjestelmä suunniteltiin yksinkertaistamaan osallistumisen valvontaa ja korvaamaan opettajien manuaaliset merkinnät taustajärjestelmään. Kun oppilaat saapuivat luokkahuoneeseen, he koskettivat NFC-tunnistetta ja läsnäolo kirjautui taustajärjestelmään. Jos kirjautumista ei tapahtunut, oppilas kirjattiin poissaolevaksi ja jos oppilas kirjautui tunnille myöhässä, myös se kirjattiin taustajärjestelmään. Mikäli poissaolo johtui esimerkiksi hammaslääkärikäynnistä, pystyi oppilaitoksen henkilökunta päivittämään järjestelmän merkintöjä. Järjestelmä esti tahalliset poissaolot informoimalla tutoreita, koulun henkilökuntaa sekä vanhempia poissaolosta reaaliajassa ja mahdollistaen näin välittömän puuttumisen. Myös turvallisuus parantui, kun oppilaiden sijainnin seuraamisesta tuli entistä helpompaa. Reaaliaikainen osallistumisluettelo oli myös opiskelijan oikeusturvana, poistaen tarpeettoman epäilyksen ja antamalla vanhemmille nopeasti tietoa valvontaan osallistumisesta. Käyttöliittymästä projektissa vastasi NextTime Solutions. (City of Oulu -project 2008, 6.)

NFC-osallistumisen valvontaan ottivat osaa myös juuri kouluaan aloittavat Hintan esikoululaiset. Projekti antoi vanhemmille reaaliaikaista tietoa lastensa osallistumisesta esikoulun tunneille. Pienissä alle 20 oppilaan ryhmissä opettajalla oli NFC-matkapuhelin osallistumisohjelmalla ja yli 20 oppilaan ryhmissä käytettiin kortinlukijaa. Oppilaat käyttivät tunneille kirjautumiseen kontaktittomia älykortteja. Kirjautumisessa rekisteröitiin oppilaan nimi ja ID, aikaleima ja suunta

(sisään tai ulos). Vanhempien oli mahdollista seurata osallistumista joko heille lähetetyistä tekstiviesteistä tai internetin kautta kansalaisportaalista. (City of Oulu -project 2008, 7.)

NFC-infokanava koulussa ja kotona käsitti aktiivisen lukujärjestyksen, kotityöt ja koulun mediasisällön. Kun oppilas kosketti älyjulistetta kotonaan tai koulussa, hän vastaanotti lukujärjestyksen ja mahdolliset luokkahuonemuutokset. Lukujärjestys sisälsi tulevat oppitunnit, tapaamiset (kuten lääkärikäynnit), mahdolliset poikkeamat (kuten edellä mainitut luokkahuonemuutokset) sekä kotityöt ohjeineen. Lukujärjestykseen oli mahdollista lisätä myös oppilaan omia opettajille tai vanhemmille näkymättömiä merkintöjä ja tapaamisia, kun lukujärjestys oli vastaanotettu. Projektin teknisestä sovelluksesta vastasi MSG Software. Koulun media sisälsi oppilaiden tuottamaa materiaalia koulun tapahtumista, juhlista tai festivaaleista, oppilaiden haastatteluista tai luokkaesittelyistä. Oppilaan koskettua NFC-tunnistetta, hän sai puhelimeensa listan, josta pystyi valitsemaan haluamansa materiaalin. Laanilan lukion aulaan oli asennettu laajakuvamonitori, jonka vieressä olevaa tunnistetta koskettamalla NFC-puhelin toimi kuten kaukosäädin, ja valittu materiaali toistettiin näytöllä. Oulun yliopiston elektroniikan ja informaatiotekniikan osasto kehitti ohjelmiston laajakuvanäytön kontrollointiin. (City of Oulu -project 2008, 6.)

3.5.5 Kirjastossa

Pohjois-Karjalan ammattikorkeakoulun kirjasto on ottanut käyttöön RFID-tekniikkaa ensimmäisenä kirjastona Pohjois-Karjalassa. Kun asiakas lainaa tai palauttaa aineistoa, välittyvät kirjoihin kiinnitettyjen RFID-tunnisteiden tiedot lukijalaitteeseen antennin avulla. Lukijalaite muuttaa RFID-tunnisteiden tiedot muotoon, jota kirjastojärjestelmä ymmärtää, minkä jälkeen tieto välittyy kirjastojärjestelmään. Tekniikan avulla onnistuu esimerkiksi pinottujen kirjojen tunnistaminen lainaus- ja palautustiskillä. Kaikki kirjat rekisteröityvät kerralla, mikä tuo asiakaspalveluun nopeutta ja tukee lainaus- ja palautusautomaattien käyttämistä. (Pohjois-Karjalan ammattikorkeakoulu 2012.)

3.5.6 Linja-autossa ja lentokentällä

Informaatio on suureksi osaksi paikka- ja sisältösidonnaista. Sen tulee olla reaaliaikaista ja vastata käyttäjän tarpeisiin esimerkiksi liikenteen informaatiopalveluissa. NFC-teknologia mahdollistaa paikkakohtaisen informaation jakamisen sekä palveluiden personoinnin laajentamisen sen mukaan, mitä tietoa käyttäjä milloinkin tarvitsee. Tämä tieto voi liittyä esimerkiksi joukkoliikenteen linjakohtaisiin aikatauluihin. (NFC-työryhmä 2011, 8.)

Linja-autossa

Joukkoliikenneinformaation jakamista käyttäjien matkapuhelimiin on kokeiltu KAMO-projektissa, joka toteutettiin Helsingissä ja Oulussa. Projektissa matkapuhelimiin oli mahdollista ottaa käyttöön Kaupunkilaisen MobiiliOpas -palvelu, josta käyttäjän oli mahdollista ladata käyttöönsä joukkoliikenteen tiedot. Projektin tavoitteena oli toteuttaa helppokäyttöinen sovellus auttamaan käyttäjien matkan suunnittelua ja matkan seurantaa. Palvelun tarkoituksena oli tarjota apuväline, joka on aina käytettävissä ja joka tarjoaa reaaliaikaiset tiedot matkan vaiheista. Sovellusta ei tarvitse hakea valikon kautta, vaan se avautuu suoraan matkapuhelimen näytölle NFC-tunnistetta kosketettaessa. Tunnisteesta on mahdollista käynnistää kännykkälipun tilaus tai pysäkkien aikataulutiedot. Tietoa voidaan jakaa samalla tavoin reaaliaikaisesti esimerkiksi erilaisissa tilaisuuksissa sekä kulttuuri- ja matkailukohteissa. (NFC-työryhmä 2011, 8 - 9.)

Esimerkiksi tietoliikenteen ja tietotekniikan keskusliitto FiCom ry on esitellyt joukkoliikenteessä käytettävää kertaluontoista eLippu-konseptiin kuuluvaa eLippua, joka mahdollistaa sähköisesti matkapuhelimeen talletettavat, aikaperustaiset lipputuotteet. Tällaisia ovat esimerkiksi kertaliput, kausiliput, ryhmäliput, tapahtumaliput tai matkailijaliput. eLippu ei kuitenkaan korvaa varsinaista matkakorttia tai mahdollista sarja- ja arvolippujen toteuttamista. Lipun matkustusoikeusaika on mahdollista asettaa heti myyntihetkellä tai ensimmäisen käyttökerran yhteydessä. Jos tapahtumalippu oikeuttaa matkustamisen jollakin tiettyllä aikavälillä, asetetaan voimassaoloaika jo myyntihetkellä. Liput on myös mahdollista lähettää etukäteen asiakkaalle tai tapahtumanjärjestäjälle, joka voi jakaa lippuja edelleen tämän jälkeen. Lippuun voi liittyä myös pääsyoikeus tapahtu-

maan esimerkiksi kortin päälle tulostettuna tai lippulajitietoon koodattuna. (FiCom ry 2008, 3 - 7.)

Lippujen tietosisältö suojataan sinetöimällä. Lipun perus-, myynti- ja voimassaolotiedoille lasketaan omat sinetit. Käytettäessä kahden sinetin mekanismia, voidaan lipun voimassaoloaika asettaa joko myyntihetkellä tai ensimmäisellä leimauskerralla. Sinettien laskennassa käytetään UID-tunnistetietoa, joka estää lipputietojen kopioimisen toiselle tuotealustalle. Sinetöintiavainta on mahdollista vaihtaa tarvittaessa versioinnin avulla. (FiCom ry 2008, 7 - 8.)

eLippu-sovellus toteutetaan mahdollisesti matkapuhelimen turvaelementille. Lipun lataaminen voi tapahtua OTA-latauksena matkapuhelinoperaattorin verkon kautta. Lipun ostaminen ja lataaminen onnistuu puhelimen selaimella tai ratkaisulla, joka pohjautuu tekstiviesteihin. Lippua käsitellään käyttötilanteessa NFC-yhteyden kautta ja asiakas voi tarkistaa lipun tiedot puhelimensa näytöltä. Matkapuhelimen eLippu-sovellus on Java-Appletti, joka toteutetaan SIM-kortille. Sovelluksen tehtävänä on hallita ja tallentaa ostettuja eLippuja. Lippupaikkoja on rajattu määrä ja niihin voidaan ladata lippuja useilta eri lipputuotteiden tarjoajilta. Asiakkaan on mahdollista selata eLippu-sovellukseen tallennettuja lippuja, valita voimassa olevia lippuja aktivoidakseen ne käyttöönsä, uusia lippuja, ostaa kokonaan uusia lippuja sekä tarvittaessa myös poistaa niitä. Talletettavien lipputuotteiden määrää kerrotaan rajoittavan lähinnä käytettävyyden hallitseminen sekä tuotealustassa oleva muistikapasiteetti. (FiCom ry 2008, 6 - 14.)

Vähintään joka kymmenennen matkapuhelimen haltijan on ennustettu käyttävän matkapuhelintaan matkalippuna tai sellaisen ostamiseen vuoteen 2014 mennessä. Juniper Research -tutkimuslaitoksen arvion mukaan matkapuhelimen välityksellä maksetaan jopa 15 miljardia lippua. Lukuun sisältyvät tavallisten matkalippujen lisäksi niin elokuva- kuin urheilutilaisuuksienkin liput. Vuoden 2011 aikana tutkimuslaitos arvioi matkapuhelimen avulla maksettavien lippujen määrän olevan noin kaksi miljardia kappaletta. (NFC-työryhmä 2011, 8.)

Lentokentällä

Maailman johtava Sveitsiläinen lentoliikenneviestinnän ja tietotekniikan asiantuntija Sita on esitellyt NFC-lähitunnistusominaisuuksien hyödyntämisen mahdollisuuksia lentokentillä. Yhtiön esittelemä ratkaisu mahdollistaa matkustajien lähtöselvityksen hoitamisen matkapuhelimen avulla. Teknologiaa olisi toiveissa päästä testaamaan käytännössä kesällä 2012. (Rinta 2012.)

Ratkaisussa matkustajien tiedot tallennetaan matkapuhelimessa olevalle SIM-kortille, jonka jälkeen kirjautuminen lennolle onnistuu yksinkertaisesti koskettamalla matkapuhelimella kirjautumista varten olevaa lukulaitetta. Yhtenä suurimmista esteistä NFC:n käytölle pidetään yhteisen standardin puuttumista. Keskustelu ongelman ratkaisemiseksi standardin luomisesta on jo aloitettu ilmailujärjestöjen kanssa. Tällä hetkellä NFC-tarroja hyödynnetään lähtöselvityksessä. Koska NFC-matkapuhelimia on vielä nykyään markkinoilla hyvin vähän, on yhtiö päätynyt tarrojen käyttöön. Tarrojen kerrotaan menestyneen käytössä hyvin. (Rinta 2012.)

3.5.7 Pysäköitäessä

NFC-lähitunnistukseen pohjautuvia parkkimittareita on jo tällä hetkellä käytössä muun muassa Yhdysvalloissa San Franciscon kaupungissa. NFC-tunnistetarroja ollaan lisäämässä kaupungissa lähes 31 000 pysäköintialueen mittariin. Kun pysäköivä asiakas haluaa maksaa pysäköinnin NFC:tä käyttäen, hän hipaisee NFC-matkapuhelimellaan mittaria, jolloin puhelin käynnistää pysäköinnin maksamiseen tarkoitetun sovelluksen. Jos maksettu aika uhkaa loppua, asiakas saa asiasta varoituksen tekstiviestillä. (Kolehmainen 2011c.)

Myös Suomessa NFC:n mahdollistamaa mukavampaa pysäköintiä on jo kokeiltu. SmartParking on Top Tunnisteen toteuttama pysäköintiratkaisu, jonka hyödyntäminen onnistuu sekä kadunvarsi- että parkkitalopysäköinnissä. Maksaminen tapahtuu matkapuhelimella ja ajoneuvoihin sekä pysäköintipaikoille kiinnitettyjä RFID-tunnisteita hyödyntäen. Maksu suoritetaan joko jälkikäteen laskuttamalla puhelin- tai luottokorttilaskulle, tai maksamalla pysäköinti jo ennakkoon.

NFC:n myötä myös pysäköinnin valvonta helpottuu, kun valvojien tarvitsee pysäköintioikeuden voimassaolon tarkistaakseen vain koskettaa NFC-matkapuhelimellaan ajoneuvon tunnistetta. (ToP Tunniste Oy 2012c.)

Älypysäköinnissä pysäköijän ei tarvitse huolehtia pysäköintiajan loppumisesta, sillä SmartParking mahdollistaa kadunvarsipysäköinnissä laskuttamisen vain todellisesta pysäköintiajasta. Järjestelmän avulla saadaan kerättyä tärkeää tietoa autopaikkojen täyttymisestä ja ihmisten pysäköintikäyttäytymisestä. Tulevaisuudessa on hyvin mahdollista, että autoilijat pystytään ohjaamaan vapaille pysäköintipaikoille joko opastaulun tai matkapuhelimen avulla. SmartParkingin ansiosta yritykset voivat kohdentaa markkinointia pysäköintialueille ja kuluttajat saavat halutessaan tarjouksia, jotka ovat sidottuja aikaan ja paikkaan. (ToP Tunniste Oy 2012c.)

SmartParking-ratkaisua testattiin Oulussa vuonna 2007. Pilottiin osallistui kahdeksan viikon ajan 50 käyttäjää. Kokeiluun osallistui myös pysäköinninvalvojia sekä Oulun Pysäköintitalo Oy. Kokeilussa kerättiin eri käyttäjäryhmiltä kokemuksia ja mielipiteitä pysäköinnin mielekkyydestä. Pilotti osoitti SmartParking-ratkaisun täyttävän sille asetetut odotukset, sillä sen käyttämisen todettiin olevan helppoa sekä pysäköinnin maksamisessa että valvonnassa. Pilotin toteuttamisessa olivat mukana ToP Tunniste Oy, Oulun kaupunki, VTT ja TeliaSonera. (ToP Tunniste Oy 2012c.)

3.5.8 Muut sovellutuskohteet

Urheilutilojen kulunvalvonta

Vuonna 2006 Oulun kaupungin koulutusosasto ja urheilutoimisto käynnistivät pilottiprojektin, jossa NFC:tä hyödyntäviä matkapuhelimia käytettiin avaimina julkisiin tiloihin. kansalaiset, jotka käyttivät Pohjankartanon koulun urheilutiloja iltaisin, saivat käyttöönsä NFC-matkapuhelimet, joilla he pääsivät liikkumaan tiloihin tiettyinä päivinä ja kellonaikoina. Tietokantaan lisättiin käyttäjien asiakastiedot, korttien ID:t, sekä pääsyinformaatio ja asiakasprofiilit päivitettiin OTA (over the air) -tekniikalla. Urheilutilan ovi avautui, kun oven vieressä olevaa luki-

jaa kosketettiin NFC-matkapuhelimella. Tavoitteena projektissa oli löytää ratkaisuja julkisten tilojen kulunhallintaan tulevaisuudessa. Projektin ratkaisun toimittivat yhteistyössä VTT ja Fara. (City of Oulu -project 2008, 4.)

Hotellihuoneen oven avaus

Mobiili kulunvalvonta on otettu käyttöön esimerkiksi hotellien ovenavauksessa. ASSA Abloy esitteli vuonna 2010 uudet matkapuhelimella avautuvat ASSA Abloy -lukot, joiden avaamiseen käytettiin tuolloin Samsung S5230 -matkapuhelinta. (Bell 2010.)

Hotellin asiakas voi hotellihuonetta varatessaan valita kirjautumiseen matkapuhelimen, johon lähetetään digitaalinen avain. Kun kirjautuminen tapahtuu digitaalisesti, matkailijan ei enää tarvitse kirjautua vastaanotossa, vaan hän voi mennä suoraan huoneeseensa. Huoneen ovi avautuu, kun matkapuhelin viedään lähelle lukkoa. Lukko tunnistaa matkapuhelimeen automaattisesti aktivoidun digitaalisen avaimen, jonka jälkeen ovi avautuu. Ovi lukkiutuu automaattisesti huoneesta poistuttaessa. Kun hotellin asiakas kirjautuu ulos hotellista, poistuu myös digitaalinen avain matkapuhelimesta. (Bell 2010.)

Iäkkäiden kansalaisten ateriapalvelut

Iäkkäiden kansalaisten ateriapalveluiden parantamista on kokeiltu pilottihankkeessa vuonna 2006. Pilotissa olivat mukana Oulun kaupungin vanhustyön palvelut, Oulun ateriapalvelut ja Oulun logistiikka. Kokeilussa käyttäjät saivat tilata aterioita soittamisen sijaan myös yksinkertaisesti koskettamalla matkapuhelimella NFC-tunnistetta. (City of Oulu -project 2008, 4.)

Vaikka joillakin käyttäjillä oli ongelmia käyttää matkapuhelinta jo perinteiseenkin tapaan, oli NFC:n käyttäminen kuitenkin suhteellisen helppo omaksua. Pilotissa ateriat tilattiin koskettamalla päivittäisistä ruokalistoista tunnisteita NFC-matkapuhelimella ja ruoat kuljetettiin kotiinkuljetuksella. Tilaukset vastaanotettiin sähköisesti Oulun ateriapalvelun tietokantaan ja ateriat valmistettiin tehdyn tilauksen mukaisesti. Oulun Logistiikka toimitti ateriat vanhuksille. Aterioiden kuljettajat antoivat raportteja NFC-teknologiaa käyttämällä aina kuljetuskierroksen alussa, onnistuneen toimituksen jälkeen, sekä kuljetuskierroksen päätyttyä.

Palveluprosessin edistymisestä saatiin reaaliaikaista tietoa ja asiakaspalvelun laatu parani. tekniset sovellukset, käyttöliittymät ja ohjelmistot tarjosi Top Tunniste ja VTT. Lisäksi VTT toteutti myös käytettävyystutkimuksen. (City of Oulu -project 2008, 4.)

Ruokaostokset kotoa matkapuhelimella

Lähikauppapalveluiden parantamista ajatellen järjestettiin vuonna 2008 Oulussa Tulevaisuuden kauppa -pilotti, jossa tarkoituksena oli testata NFC:tä hyödyntävää palvelua, joka mahdollistaa ostosten tekemisen kotoa käsin ilman monimutkaista tietokoneen tai mobiililaitteen käyttöä. Ensisijaisena tarkoituksena pilotissa oli helpottaa vanhustyötä. (Kalliokoski 2008.)

Pilotissa ostajan oli mahdollista valita kotonaan tuotekirjasta haluamansa tuotteet ja tilata ne NFC-matkapuhelimella. Järjestelmä välitti tilaustiedot kauppaan, joka käsitteli tilauksen ja toimitti tuotteet seuraavana päivänä. Tilaussovelluksen ja kaupan tilausjärjestelmän suunnitteli ja toteutti TeliaSonera. Lisäksi pilotin toteutukseen osallistuivat Oulun kaupunki, Oulu Innovation, Tradeka ja Lintulammen asukasyhdistys. (Kalliokoski 2008.)

Diabeetikoiden terveydentilan seuranta

NFC-rajapintaa käyttävien laitteiden avulla voidaan seurata terveydentilaa esimerkiksi pikatestien, ihonpäällisten antureiden ja monitorien avulla, sekä saada nämä tiedot esimerkiksi vain lääkärin käyttöön koskettamalla kohdetta matkapuhelimella. (Seppä 2011, 18.)

Vuonna 2008 Oulun omahoitohanke pilotoi yhteistyössä ProWellness Oy:n kanssa verensokerimittauskokeilun NFC-rajapintaa hyödyntäen. Käyttämällä VTT:n kehittämää NFC-kommunikoinnilla varustettua kaupallista verensokerimittarin prototyyppiä, projekti tarjosi diabetespotilaille taustatukea itsehoidon parantamiseen. Mittarin ja NFC-puhelimen avulla verensokerimäärän mittaustulokset lähetettiin Oulun itsehoitoportaalin itsehoitosysteemiin. Tulosten saavuttua systeemi palautti täsmälliset ohjeet insuliinin annosteluun. Projektin tavoitteena oli arvioida, vähentääkö NFC-systeemi tarvetta terveydenhoidon henkilökunnan osalta diabeteshoidon alkuvaiheessa. (City of Oulu -project 2008, 11.)

Ääniviestit ja puhuvat tuoteselosteet heikkonäköisten ja näkövammaisten avuksi

Ikääntyvien kansalaisten osuus yhteiskunnassa kasvaa jatkuvasti, jolloin heidän tarpeensa korostuvat yhä entistä enemmän. Tuotteiden digitaaliseen tuotetietoon linkittävät ratkaisut ovat tällä hetkellä yleistymässä, koska sekä näkevät että näkövammaiset henkilöt voivat hyötyä niistä monin eri tavoin. Tekniikka mahdollistaa ihmisen toiveiden mukaisen tiedonsaannin esimerkiksi elintarvikkeiden alkuperästä, ekologisuudesta tai allergisoivista aineista. (VTT 2012.)

Heikkonäköisten ja näkövammaisten elämää helpottamaan on kehitetty HearMeFeelMe-hankkeessa NFC-teknologiaa hyödyntäen viisi erilaista sovellusta lääketietojen saamiseen. Tavaroiden merkitsemistä ja tunnistamista ääniviestien ja puhuvan tuoteselosteen avulla on testattu lääke- ja elintarvikepakkauksissa kohderyhmään kuuluvien kotona. Kun NFC-lukijalla varustetulla matkapuhelimella kosketetaan paketin tunnistetarraa, voidaan käyttäjälle esittää tunnisteen sisältämä tuotetieto, kuten lääkkeen nimi ja annosteluohje, äänenä joko tietokoneen tai matkapuhelimen kaiuttimen kautta. (VTT 2012.)

Käyttäjäkokeissa kaikkein suosituimmaksi sovellukseksi osoittautui ToP Tunnisteen Touch n' tag -demo. Sovelluksessa näkövammaisten oli mahdollista liittää kotona oleviin esineisiin ja elintarvikkeisiin omia ääniviestejä. Kun käyttäjä koskettaa NFC-matkapuhelimellaan tunnistetarraa, hänellä on mahdollisuus äänittää sille haluamansa ääniviesti matkapuhelimella. Jatkossa viestien kuunteleminen onnistuu koskettamalla matkapuhelimella tarraa uudelleen. Kokeilussa selvisi, että useimmiten merkatut tuotteet olivat ruokapakkauksia. Laitteesta todettiin olevan hyötyä asioiden tunnistamisessa ja tuotetietojen saamisessa. Käyttäjät pitivät siitä, että he pystyivät laatimaan ja liittämään tavaroihin omanlaisensa viestin. (VTT 2012.)

Hankkeessa kehitettiin myös puhuva lääkepaketti -demo. Ideana on, että lääkepaketin NFC-tarralle tallennetaan lääkkeen tiedot apteekissa. Tämän jälkeen käyttäjän on mahdollista koskettaa lääkepakettia matkapuhelimellaan, jolloin hän kuulee annosteluohjeet ja muut lääkkeen tiedot äänimuodossa. Toistaiseksi demo toimii ainoastaan PC:ssä. (VTT 2012.)

Hankkeessa syntyi myös muun muassa vielä allakkademosovellus, jonka tarkoituksena on vahvistaa vanhuksen lääkkeiden ottamisen sosiaalisen verkoston tukea. Ajatuksena on, että hoitajat ja omaiset luovat muistutuksia esimerkiksi lääkehallinnan tai tapaamisten muistamisen tueksi. Kun käyttäjä saa muistutuksen, hän kuittaa sen koskettamalla matkapuhelimella esimerkiksi lääkeannostelijaa. Tällöin omaisten ja hoitajien tietoon välittyy, että lääke on otettu. (VTT 2012.)

Näkövammaiset ovat valmiita ottamaan NFC:n käyttöönsä tulevaisuudessa erityisesti tavaroiden tunnistamisessa, puhuvana tuoteselosteena, päivyrinä, henkilökohtaisena muistiona, sekä esimerkiksi omakohtaiseen kodinkoneiden käytön ohjeistukseen. Tiedostojen muuttamisessa äänimuotoon ei ole VTT:n mukaan ongelmia, mutta nykyinen laitekanta ei ole kehittynyt tarpeeksi uusimpien NFC-sovellusten käyttöönottamiseksi. Toistaiseksi ei vielä ole matkapuhelinalustoja, joille kehitetyt ratkaisut olisi tarkoitettu. Projektin loppukäyttäjinä olivat Oulun 6. Joutsen apteekki, Näkövammaisten keskusliitto, Caritas-Säätiö sekä espanjalainen SSI, joka tuottaa vanhuspalveluja. VTT:n lisäksi hankkeessa olivat mukana kotimainen ToP Tunniste, kreikkalainen Demokritos ja espanjalainen Tecnalia. (VTT 2012.)

Älyvaatteet parantamaan palvelukodin valvontaa

Elektroniikan seuraava askel on puettava tietotekniikka. Sydämen sykkeen tai muiden elintärkeiden signaalien mittaamiseen voidaan käyttää avuksi älypaitaa, jonka sisään on sulautettu sensoreita. Tiedot voidaan lähettää integroidulla antennilla joko käyttäjän omaan päätteeseen tai suoraan sairaalaan. Tulevaisuudessa potilaat voivat jäädä kotiinsa, kun heidän tilaansa voidaan seurata tarkasti ja tarvittava apua voidaan lähettää heti, kun sellaselle tulee tarvetta. (Kemiläinen 2012.)

Päälle puettavia antenneja voidaan hyödyntää tulevaisuudessa telelääketieteen lisäksi esimerkiksi kulunvalvonnassa. Antennit ovat jo hyvin tunnettuja ja tutkittuja, mutta perinteisesti ne ovat sopineet vain katoille tai mastoihin. Ihmiskeho absorboi suurimman osan energiasta tehden radiolinkin tehottomaksi. Linkkiä

voidaan tehostaa älykkäällä suunnittelulla. Ihmiskeho voi toimia parhaimmillaan jopa passiivisena osana antennia. Käyttäjän koko ja asento näyttelevät suurta roolia antennin ominaisuuksista, kun käytössä on tavallisen FM-radiolähetyksen taajuus (100 MHz). Toisaalta GPS-antenni voidaan sijoittaa myös selkään tai ranteeseen. Hyvän yhteyden kannalta on merkitystä sillä, kuinka kaukana antenni ja keho sijaitsevat toisistaan. Kun antennin ja kehon välissä on metallieriste, keho ei pääse vaikuttamaan antennin toimintaan. Eriste tekee kuitenkin antennista suurikokoisen ja kömpelön. Helpointa on valmistaa yksinkertainen yksikerroksinen antenni, jossa ei ole metallieristettä. Tällöin antenni on puettava riittävän etäisyyden päähän kehosta. Esimerkiksi GPS-antenni tulisi sijoittaa muutaman senttimetrin päähän kehosta. Etäisyys voi tuntua pitkältä, mutta ihmisen ulkovaatetus on yleensä tarpeeksi paksu ja väljä tähän tarkoitukseen. (Kemiläinen 2012.)

Kellomäki suunnitteli osana väitöskirjaansa tunnistustarra-antennin, joka puetaan henkilön paidan kaulukseen. Antennia voidaan käyttää esimerkiksi vanhustenkodin kulunvalvonnassa. Jos esimerkiksi muistisairas potilas kävelee ulos ulko-ovesta, tarra laukaisee hälytyksen. Konsepti on samanlainen kuin jokaisesta supermarketista löytyvissä varashälyttimissä, mutta nyt tarra on mahdollista pukea mukavasti vaatteisiin. (Kemiläinen 2012.)

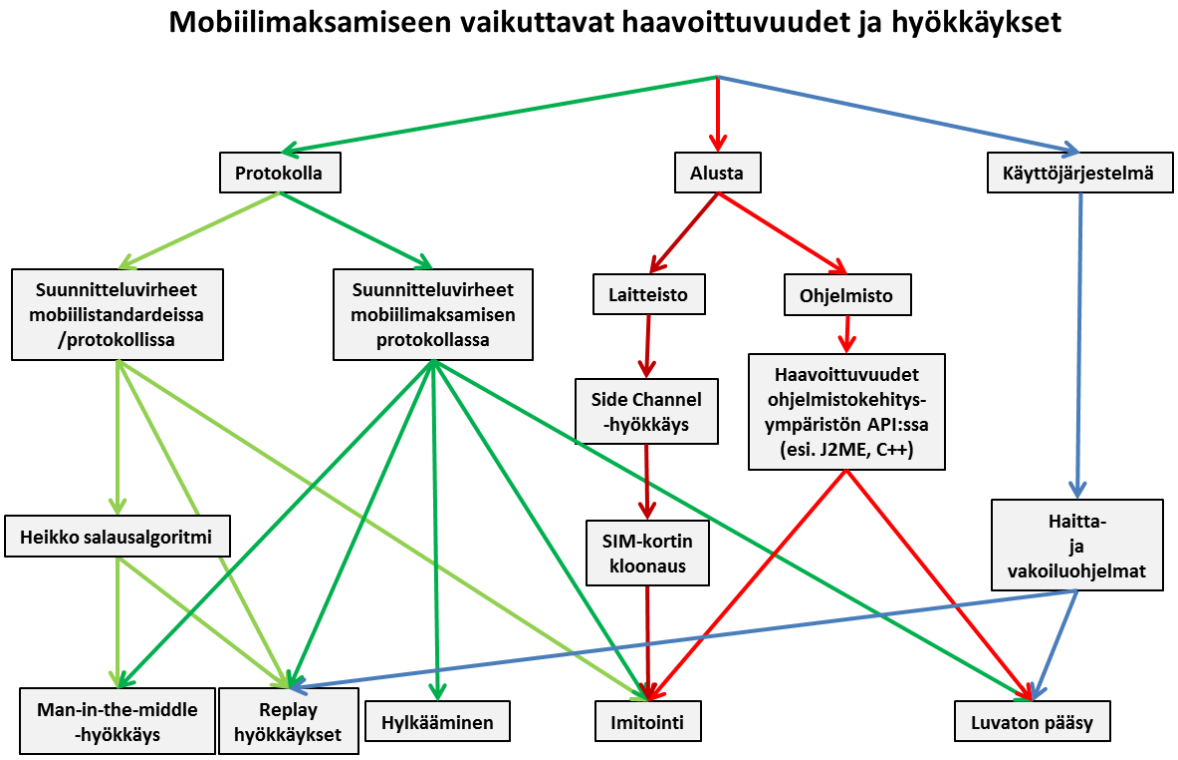
Sairaalatekniikan huollon raportointi

Suomessa on kehitetty ratkaisu sairaalatekniikan huollon raportointiin Sofor Oy:n ja TOP Tunniste Oy:n toimesta. Ratkaisussa huoltohenkilöt kirjautuvat huoltokohteisiin NFC-matkapuhelimen avulla ja huollon jälkeen kuittaavat tarkastuksen ja valmistuneen huoltotoimenpiteen. Matkapuhelimella on mahdollista ottaa myös kuvia ilmenneistä vioista. Raportointi yksinkertaistuu, kun tekstin kirjoittamisen sijaan raportointiin riittää tunnisteen koskettaminen ja yhtiön tietojärjestelmä vastaanottaa kaiken lähetetyn tiedon reaaliajassa. (NFC-työryhmä 2011, 7.)

3.6 NFC:n tietoturvauhat

NFC:tä käytetään usein arkaluontoisten tietojen välitykseen, kuten esimerkiksi tunnistamiseen ja maksamiseen. Tämän vuoksi tekniikan tietoturvaongelmia on syytä analysoida erittäin tarkasti. NFC:n suojamekanismit ovat usein ulkoisia tekijöitä. (Kainulainen 2011.)

Kuvassa 15 havainnollistetaan mobiilimaksamisen tietoturvallisuuteen vaikuttavia komponentteja. Monien eri osapuolten tekniikan tietoturvallisuus on otettava huomioon, jotta NFC-yhteydellä siirrettävän tiedon suojaaminen onnistuu. Vaikka itse NFC-tekniikan tietoturva olisikin kunnossa, voi hyökkäys kohdistua esimerkiksi alustana käytettävän laitteiston tai ohjelmistojen heikkouksiin. (Kainulainen 2011.)



Kuva 15. Mobiilimaksamisen tietoturvaan vaikuttavat komponentit (Kainulainen 2011).

3.6.1 Urkinta

NFC:n käytössä on vaarana, että tekniikka paljastaa henkilöstä liikaa tietoja. Sirut voivat sisältää runsaasti henkilötietoja ja tiedot on mahdollista lukea salaa, joten mahdollisuus tietojen joutumisesta vääriin käsiin on olemassa oleva, mutta myös tiedostettu ongelma. (Foley 2012.) NFC:n turvaominaisuuksiin ei voida täysin luottaa siitä huolimatta, että kahden laitteen välinen yhteys vaatiikin hyvin pienen välimatkan (toiminta-alue noin 4 senttimetriä). Signaalin poimiminen on mahdollista antennilla, koska yhteys on langaton. Jotta signaalin poimiminen onnistuu, on hyökkääjän oltava muutaman metrin päässä yhteydestä. Tämä kuitenkin tuskin tuo yhteyden urkintaan ongelmia. Jos urkkija seisoo jonossa NFC-tekniikkaa käyttävän maksajan takana, tuskin kukaan epäilee hänen poimivan edellä olevan maksutunnuksia lennosta. (Kainulainen 2011.)

Yksityisyyden suojan puolustajat kutsuvat RFID-siruja ”vakoilusiruiksi”, koska kuka tahansa oikeaan aikaan oikeassa paikassa oleva henkilö voisi kopioida sirun tiedot RFID-lukulaitteella ja halutessaan käyttää näitä tietoja erilaisiin yksityisyyttä loukkaaviin tarkoituksiin, kuten vakavaan identiteettivarkauteen tai vakoiluun. Sirun tiedoilla voidaan myös seurata ihmisiä, kuten viranomaisia tai yksityishenkilöitä, ja pahimmillaan sirun omistajan turvallisuus voi vaarantua. Myös kansalaisoikeuksien menettämistä on pelätty, kun mahdollisuus yhä entistä tarkempaan valvontaan kasvaa. (Foley 2012.)

RFID:n kannattajien mukaan kaikkiin teknologioihin on aina suhtauduttu ja tullaan suhtautumaan aluksi varauksella ja vastentahtoisesti. RFID:hen liittyviä samoja väitteitä on esiintynyt myös silloin, kun viivakoodit tulivat käyttöön. Esimerkiksi Yhdysvalloissa arviolta 30 - 40 miljoonaa ihmistä kuljettaa mukanaan jatkuvasti RFID-sirua. Tietoon ei vielä ole tullut tapauksia, jossa yksityisyyden suojaa olisi loukattu. Jotkin asiantuntijat pitävät vaaraa matkapuhelinten jäljittämisestä paljon suurempana, sillä useimmista RFID-siruista poiketen niissä on aina oma virtalähde, joka mahdollistaa niiden seuraamisen pitkien matkojen päästä. RFID-sirun lukeminen edellyttää pääsemistä lukijalaitteen kanssa alle metrin etäisyydelle. Jotkin yritykset ovat ottaneet huomioon ihmisten huolen yksityisyyden menettämisestä. Nämä yritykset ovat lisänneet pakkauksiin tai

käyttöohjeisiin tiedon siitä, kuinka RFID-siru tehdään toimintakyvyttömäksi tai poistetaan kokonaan. Useimmat asiantuntijat ovat kuitenkin sitä mieltä, että RFID-siruista ei tule olemaan uhkaa ihmisten oikeuksille. (Foley 2012.)

3.6.2 Inhimillinen riski

NFC-matkapuhelinten ja NFC-korttien käyttäjien huolimattomuus synnyttää inhimillisen tietoturvariskin. Jos käyttäjä unohtaa matkapuhelimensa tai korttinsa julkiselle paikalle, saattaa joku halutessaan varastaa käyttäjän tiedot itselleen. Pelkkä PIN-koodi ei riitä tämänkaltaisilta tietoturvariskeiltä suojautumiseen, vaan tällöin tarvitaan useampia kuin yksi tunnistautumiskeinoja. (Kainulainen 2011.)

3.6.3 Tiedon muokkaus

On mahdollista, että hyökkääjä pyrkii tuhoamaan tietoja NFC-laitteelta käyttäen hyväkseen RFID-jammeria, joka on häirintään tarkoitettu radiolähetin. Tähän uhkaan ei ole vielä löydetty aukotonta ratkaisua, mutta NFC-laite voi tehdä yhteyden aikana tarkistuksia, joiden avulla voidaan havaita, mikäli hyökkäystä yritetään. Tiedon muokkaaminen on erittäin vaikeaa, koska hyökkääjän on suoritettava se bitti kerrallaan. Miller-koodausta ja 100 prosenttista modulaatiota käytettäessä on mahdollista muokata vain joitakin bittejä. Signaalista pystytään poistamaan tauot käyttämällä 100 prosenttista modulaatiota. Tästä huolimatta taukoa ei voida luoda paikkaan, jossa sitä ei ole ollut jo ennestään. Bittijonosta voidaan muokata tämän vuoksi vain 11 jälkimmäistä bittiä. Kaikkien bittien muokkaaminen onnistuu Manchester-koodausta käyttävällä siirrolla 10 prosentin modulaatiolla. Yhteyteen on mahdollista myös yrittää syöttää jotakin ylimääräistä tietoa. Tämä onnistuu kuitenkin vain, jos kohteelta vaaditaan pitkä aika vastaukseen aloitteentekijälle. Näin ollen hyökkääjä pystyy vaikuttamaan sisältöön lähettämällä yhteyteen omaa tietoaan. Lähetyksen on kuitenkin tapahduttava ennen kuin alkuperäinen kohde aloittaa oman vastauksensa lähettämisen. (Kainulainen 2011.)

3.6.4 Haitalliset tunnisteet

NFC-tunnisteita voidaan lukea NFC-tekniikkaa tukevilla laitteilla. Tunnisteet suorittavat matkapuhelimessa niille määriteltyjä tietynlaisia toimintoja, kuten avaavat jonkin tietyn internetsivun tai hakevat bussiaikatauluja sovelluksen avulla. Vaarana on, että hyökkääjä muokkaa oikeaa tunnistetta, tai asettaa tilalle uuden tunnisteen, joka on määritelty ajamaan matkapuhelimessa haitallisia toimintoja. Huijaamalla käyttäjä voidaan saada suorittamaan erilaisia haitallisia toimintoja, kuten avaamaan haitallisia internetsivustoja tai soittamaan puheluita. Haitallisen internetsivun voi naamioida helposti, kun sivun otsikkoon ja haitallisen osoitteen URI-kenttään asetetaan julkinen osoite. (Kainulainen 2011.)

3.6.5 Linkkihyökkäys

Linkkihyökkäystä (relay attack) kutsutaan Man in the Middle -hyökkäykseksi. Hyökkäyksessä hyökkääjä välittää tietoa eri osapuolten välillä. Hyökkääjän laite korvaa aidon laitteen, kerää lähteen yhteysohjeita ja lähettää ne eteenpäin oikealle laitteelle. Hyökkääjän laite kerää aidolta laitteelta tulevat vastaukset ja välittää ne takaisin lähteelle. Tämä hyökkäyskeino on toteutettavissa helposti yksinkertaisella laitteistolla, koska laitteiden ei tarvitse käsitellä kuin modulaatiota. Modulaatiotekniikat, joita NFC-tunnisteet käyttävät, löytyvät ISO14443/ISO18092-standardeissa. Tämä helpottaa hyökkäykseen sopivan laitteen valintaa. Man in the Middle -hyökkäys aiheuttaa yhteydessä aina hieman viivettä, jolloin näitä hyökkäyksiä voitaisiin estää asettamalla yhteysajoille lyhyet aikarajat. (Kainulainen 2011.)

3.6.6 Haittaohjelmat

NFC-tunnisteisiin liittyy useita tietoturvauhkia. Kun käyttäjä lukee matkapuhelimellaan tunnisteen, voi muunneltu tunniste ajaa matkapuhelimeen koodia joltakin sivustolta ja asennuttaa laitteeseen viattomaksi naamioidun ohjelman. Hyökkäyssivuston osoite voidaan piilottaa URI-kenttään, joka ohjaa laitteen

madon lataamista varten tehdylle sivustolle. Puhelin ei varoita latauksesta, jos käytetään Silent MIDlet -asennusta. Suoritus voi olla piilossa väärien komentokäskyjen takana. Kun haittaohjelma on päässyt laitteeseen, pääsee mato levittäytymään vapaasti esimerkiksi NFC-yhteyksien kautta. (Kainulainen 2011.)

3.6.7 Suojautuminen

Monen eri osapuolen on otettava NFC-tekniikan tietoturva huomioon, mikäli NFC-yhteydessä siirrettävä tieto halutaan saada suojatuksi. Laitteet tulisi suojata laitevalmistajien toimesta kryptografisilla (salakirjoitus) protokollilla, jotta autentikoinnin (todennuksen) ja tiedonsiirron turvallisuus saadaan varmistettua. Käyttäjätunnuksien on oltava lukittuna vahvoilla salasanoilla, jonka lisäksi tarvitaan asianmukaiset näyttölukitukset sekä virus- ja palomuuriohjelmat. Myös sovelluskehittäjien on otettava sovelluksissa huomioon tietoturvallisuus mahdollisimman hyvin ja pyrittävä varmistamaan, että sovellukseen ei pääse kolmatta osapuolta ajamaan haitallisia koodeja. Maksutapahtuman osapuolten on määriteltävä turvalliset siirtostandardit ja toimenpiteet vahvan tietoturvatason saavuttamiseksi. (Kainulainen 2011.)

Matkapuhelimeen on mahdollista lisätä erillinen turvaelementti tai -siru. Vaihtoehtoisesti voidaan hyödyntää myös matkapuhelimen suoritinta (CPU). Turvallisuuden lisäämiseksi voidaan käyttää myös matkapuhelimen väärinkäytöltä suojaavaa turvallista muistikorttia, sekä uudenlaista UICC-SIM-korttia. (NFC-työryhmä 2011, 11.)

Laitteen NFC-yhteyksien turvallisuuteen vaikuttaa todella paljon käytössä olevan käyttöjärjestelmän turvallisuus. Symbian C++ ja J2ME (Java Micro Edition) -ympäristöjen rajapinnat tunnetaan heikoiksi, sillä ne päästävät hyökkääjän toimintoihin, jotka ovat muutoin rajattuja. J2ME tarjoaa SATSA (Security and Trust Services API) -laajennuksen tilanteisiin, joissa SIM-korttia käytetään mobiilimaksamisessa ja muissa erikoistilanteissa. (Kainulainen 2011.)

Turvallisuusluokitukseltaan korkeampaan tasoon pääsee vain syöttämällä PIN-koodin, joka ei ole sama kuin puhelimen avaamiseen tarvittava koodi. Jos tätä hyödynnetään NFC-yhteydessä, on hyökkääjän ensin murrettava PIN-koodi päästäkseen avaamaan yhteys. (Kainulainen 2011.) Lähimaksaminen onkin yhtä turvallista kuin sirukortilla maksaminen. Turvallisuutta voidaan lisätä myös sillä, että PIN-koodia kysytään kortin haltijalta säännöllisin väliajoin, esimerkiksi joka kymmenennen ostokerran yhteydessä. Jos kortti joutuu vääriin käsiin, loppuu maksaminen viimeistään PIN-koodia pyydettäessä. (Luottokunta 2012e, 2.) Monissa matkapuhelimissa on PIN-koodin lisäksi myös muita turvallisuusominaisuuksia, kuten digitaalinen allekirjoitus, biometrinen tunnistautuminen ja salauksen purku (Kainulainen 2011).

Kaikista tärkein suojautumiskeino hyökkääjiä vastaan on standardointi:

> "NFC-tekniikan siirtoyhteydelle on tällä hetkellä kaksi standardia; ISO/IEC 18092 / ECMA-340 Near Field Communication Interface and Protocol-1 (NFCIP-1), sekä ISO/IEC 21481 / ECMA-352 Near Field Communication Interface and Protocol-2 (NFCIP-2).
>
> Esimerkiksi NFCIP-1 määrittelee siirrossa käytettäviksi perusmekanismeiksi seuraavat: Elliptic Curve Diffie-Hellman (ECDH) Key exchange [192 bittiä], key derivation and confirmation [128 bittinen AES], data encryption [128 bittinen AES], data integrity [128 bittinen AES].” (Kainulainen 2011.)

NFC on yhteensopiva ISO/IEC 14443 -x (Identification cards - Contactless integrated circuit cards - Proximity cards) -standardisarjan kanssa, joka määrittelee niiden älykorttien ominaisuudet ja tiedonsiirron, jotka toimivat 13,56 MHz:n taajuudella. (Kainulainen 2011.)

NFC-tekniikka yleistyy nopeasti, joten monet laitevalmistajat ovat ottaneet tarkasti huomioon NFC:n tietoturvallisuuden. Tulevaisuudessa tullaan näkemään tietoturvaa parantavia uusia, kehittyneempiä ratkaisuja. Mobiilimaksaminen on toimenpiteenä erittäin turvallisuuskriittinen, joten luottoyhtiöt ja pankit vaativat uuden teknologian käyttöönotossa tiukkoja turvamekanismeja. (Kainulainen 2011.)

Luottokunnan mukaan maksukorttiyhtiöt ja pankit luottavat NFC-tekniikkaan jo suurelta osin. Eurooppaan on laskettu liikkeelle miljoonia lähiluettavia kortteja.

Korttien tietoturvasta kerrotaan huolehdittavan monin tavoin. NFC-kortti on vietävä hyvin lähelle maksupäätettä, eikä veloitus onnistu lompakossa olevasta kortista. Lyhyessä ajassa tapahtuvien peräkkäisten veloitusten määrää on rajoitettu, jonka lisäksi tiedonsiirto tapahtuu salattuna. Kortilla voi maksaa ilman PIN-koodia korkeintaan 25 euroon asti, jonka jälkeen suuremmat ostokset on maksettava perinteisellä tavalla sirulukijan kautta. Kuluttaja ei ole vastuussa kortistaan enää sen jälkeen, kun on ilmoittanut sen kadonneeksi. (Lehto 2012.)

3.7 NFC -teknologian kehittymisen haasteita

NFC-teknologiaan liittyy haasteita, jotka ovat hidastaneet NFC:n käyttöönottoa. Teknologian on oltava toimintavarmaa ja luotettavaa, ennen kuin sen käyttö voi lisääntyä.

3.7.1 Lainsäädäntö ja standardit

NFC-teknologian yleistymisessä suurimpana haasteena ei ole enää nykyaikana ollut teknologia, vaan kehittymättömät standardit ja säännökset. Teknologia on ollut jo kymmenen vuoden ajan käyttövalmis, mutta siihen ei ole uskallettu investoida lakien ja standardien puuttumisen vuoksi. (Seppä 2011, 6.)

Nykyinen lainsäädäntö ei estä NFC-teknologian käyttöönottoa, mutta ei myöskään kannusta siihen. Tulevaisuudessa lainsäädäntöön voi ilmetä uusia tarpeita esimerkiksi kuluttajansuojaan tai tietoturvaan liittyen. Kehitystä tulee seurata. (NFC-työryhmä 2011, 12.)

3.7.2 Tekniikka

NFC-laitteiden käyttämien taajuuksien saatavuuden suhteen ei ole ongelmia. Taajuuksien saatavuus ei hidasta tekniikan kehittymistä, koska NFC- ja muiden etätunnistuslaitteiden käyttämä taajuus 13,56 MHz on vapautunut radioluvista. (NFC-työryhmä 2011, 12.)

13,56 MHz:n taajuuden tiedonsiirtonopeus (106, 212 tai 424 Kbit/s) soveltuu pienten tietomäärien siirtoon. Jos käsiteltävänä on suurempia tietomääriä, voidaan NFC:tä käyttää yhteyden avaamiseen, jonka jälkeen varsinainen tiedonsiirto hoituu toisella tekniikalla. (NFC-työryhmä 2010, 6.)

ERC Recommendation 70 - 03 -suosituksessa (ns. SRD-suositus, Short Range Devices) on määritelty Euroopassa käytettävät lyhyen kantaman radiolaitteiden tekniset parametrit. Lisäksi SRD-suosituksessa määritellään tekniset parametrit induktiivisille laitteille, jotka toimivat muun muassa 13,56 MHz:n taajuudella. Taajuuksien käytöstä on määrätty EU-maissa myös Euroopan komission päätöksellä 2009/381/EY. Induktiivisia laitteita saa SRD-suosituksen ja Euroopan komission päätöksen mukaisesti käyttää Suomessa. (NFC-työryhmä 2010, 6 - 7.)

Taajuus 13,56 MHz kuuluu niin sanottuun ISM-kaistaan (Industrial, Scientific and Medical applications). ISM-sovelluksia ovat esimerkiksi teollisuusympäristön suuritehoiset kuumentimet, joita käytetään tyypillisesti huonekalu- ja rakennusmateriaaliteollisuudessa. Radioliikenteen on hyväksyttävä häiriöt, joita ISM-sovellukset mahdollisesti aiheuttavat. (NFC-työryhmä 2010, 7.)

3.7.3 Erityisryhmät

Uutta tekniikkaa käyttöönotettaessa on kiinnitettävä huomiota myös heikkojen kuluttajaryhmien asemaan. Uuden tekniikan hyödyntäminen voi tuottaa hankaluuksia esimerkiksi iäkkäille kuluttajille. Tällöin on tärkeää, että palveluita voidaan käyttää myös perinteisempään tapaan. (NFC-työryhmä 2011, 13.)

Myös alaikäiset kuluttajat on otettava huomioon. Alaikäiset tarvitsevat tekemiinsä oikeustoimiin usein huoltajiensa suostumuksen. Tarvetta suostumukseen arvioidaan muun muassa maksajan iän ja ostoksien laadun ja hinnan mukaan. Sitoutumista velkasuhteeseen ei koskaan voida katsoa merkitykseltään vähäi-

seksi oikeustoimeksi. Hyödykkeen laadun suhteen katsotaan, onko hyödyke tavanomainen ostos alaikäiselle. (NFC-työryhmä 2011, 13.)

Kun uutta tekniikkaa otetaan käyttöön, on varmistettava, että alaikäiset pystyvät tutustumaan vain materiaaliin, joka sopii heidän ikätasoonsa ja että he pystyvät tekemään vain ostoksia, jotka ovat heille mahdollisia. Jotta palveluille voidaan asettaa ikärajoituksia, on sopijakumppanin henkilöllisyyden tunnistamisella olennainen merkitys. Tähän vaaditaan vahvaa sähköistä tunnistamista. (NFC-työryhmä 2011, 13.)

3.7.4 Vastuu palveluiden toimittamisesta

Jotta NFC-tekniikan käyttö voi lisääntyä, on sen oltava toimintavarmaa ja luotettavaa. On kuitenkin mahdollista, että tekniikan viimeistelystä huolimatta käytössä esiintyy erilaisia toimintahäiriöitä ja järjestelmävirheitä. Mahdolliset virheet voivat heikentää käyttäjien luottamusta tekniikkaa kohtaan, mikäli ei tiedetä kuka vastaa mahdollisesti koituvista vahingoista. Huolta saattaa aiheuttaa esimerkiksi se, onko mahdollista, että kontaktittomassa maksamisessa veloitus tapahtuisi useita kertoja. Myös se voi aiheuttaa huolta, jos sirulta voidaan viedä tietoa tai veloittaa sitä huomaamattomasti. (NFC-työryhmä 2011, 12.)

Kun kuluttaja tulevaisuudessa ostaa esimerkiksi pääsylippua konserttiin siirtymällä julisteessa olevan NFC-tunnisteen kautta verkkokauppaan, jossa ostoprosessin aikana tapahtuukin jokin virhe, eikä maksaja tällöin saakaan ostamaansa lippua veloituksesta huolimatta. Tilanteessa voi olla mahdotonta selvittää, onko virhe johtunut matkapuhelimen, lukijalaitteen, vai ehkä palveluntarjoajan järjestelmän virheestä. Tällaisten ongelmien vuoksi täytyy sopia yhteiset toimintatavat tai viimekädessä myös lainsäädäntö, jotta tiedetään, kuka on vastuussa mahdollisista ongelmista. Koska NFC-matkapuhelinta tullaan todennäköisesti käyttämään erittäin laajasti maksamiseen ja tiedonsiirtoon, on suositeltavaa käyttää standardiratkaisuja, jolloin alustojen ja ratkaisujen välille pääsee syntymään kilpailua. (NFC-työryhmä 2011, 12 - 13.)

4 Yhteenveto

Vielä tänä päivänäkin lähimaksamisessa käytetään myös etämaksumenetelmiksi luettavia ratkaisuja. Yleisimmät näistä ovat tekstiviestillä tai puhelinsoitolla maksaminen. NFC-teknologia on tehnyt tuloaan uutena ratkaisuna lähimaksamiseen jo vuosia, mutta Suomessa tämä maksutapa on alkanut yleistyä todenteolla vasta vuoden 2012 aikana, kun maksupäätteiden ja maksukorttien uudistuessa niistä löytyy yhä useammin myös lähimaksuominaisuus. NFC-matkapuhelinten käyttäminen maksamisessa lisääntyy, kun markkinoilta löytyy entistä monipuolisemmin NFC-maksamista tukevia malleja. Myös matkapuhelimeen liimattaville tunnistetarroille voi löytyä kysyntää, jos ei haluta käyttää kontaktitonta maksukorttia, eikä matkapuhelimen oma tekniikka tue maksamista. Jo jonkin aikaa kehitteillä ollut NFC-SIM-kortti voi tuoda onnistuneesti toteutuessaan NFC-maksamisen mahdolliseksi lähes jokaisessa matkapuhelimessa ja vauhdittaa näin osaltaan NFC maksamisen yleistymistä.

Kontaktiton lähimaksu tuo pienten kertaostosten maksamiseen kaivattua lisänopeutta ja helppoutta. Maksun molemmat osapuolet hyötyvät, kun kassoilla asioiminen nopeutuu ja maksamisesta koituvat kulut pienenevät käteismaksujen ja perinteisten korttien käytön vähentymisen myötä. Jotta kuluttajat ryhtyvät käyttämään NFC-teknologiaa, sen on oltava helppokäyttöistä, turvallista, helposti saatavilla ja toimintavarmaa. Teknologian käyttöönotossa on myös muistettava ottaa huomioon erityisryhmät, kuten alaikäiset kuluttajat ja henkilöt, joilla ei ole valmiuksia uuden tekniikan omaksumiseen.

Lähimaksamisen tietoturvallisuus herättää vielä jonkin verran epävarmuutta. Kun teknologiaa käytetään maksamiseen, siltä vaaditaan tiukkoja turvallisuusmekanismeja. Tietoturvallisuus on jo otettu hyvin huomioon useiden eri tahojen toimesta ja se on huomioitu tarkasti ennen kuin lähimaksamista on ryhdytty ottamaan käyttöön laajemmin. Aina on kuitenkin otettava huomioon mahdollisuus, että tekniikan viimeistelytyöstä riippumatta käytössä esiintyy odottamattomia ongelmia. Näiden varalta on tiedettävä jo etukäteen, että kuka vastaa mistäkin. Tulevaisuudessa tietoturvallisuus tulee vielä paranemaan entisestään uusien ja entistä kehittyneempien ratkaisujen myötä. Jo tällä hetkellä pankit ja maksukort-

tiyhtiöt luottavat NFC-teknologiaan, eikä sitä käytettäessä ole vielä tullut ilmi väärinkäyttötapauksia, vaikka teknologia on ollut jo jonkin aikaa laajalti käytössä muualla maailmassa myös maksutapahtumissa. Myös Suomessa sitä hyödynnetään entistä enemmän erilaisissa sovellutuskohteissa.

5 Pohdinta

Ennen opinnäytetyötä en ollut koskaan aikaisemmin kuullut NFC-teknologiasta. NFC on vielä tällä hetkellä sen verran uusi ja vasta yleistymässä oleva teknologia, ettei Suomessa ole ehtinyt edes vakiintua käyttöön mitään virallista termistöä. Maksutilanteissa voidaan puhua esimerkiksi lähimaksamisesta (jota käytetään luultavasti kaikkein eniten), kontaktittomasta maksamisesta tai pikamaksamisesta. Maksutapaa on kutsuttu joissakin tilanteissa myös etämaksamiseksi, mutta tämä termi on harhaanjohtava. Ennen aiheeseen tutustumista en ollut koskaan tullut ajatelleeksi, että matkapuhelimella suoritettavien pienten tekstiviesti- ja puhelinsoittomaksujen lisäksi myös kontaktiton maksaminen ilman tunnistautumista esimerkiksi kaupassa voisi onnistua vain lähimaksukorttia tai peräti matkapuhelinta näyttämällä. Aihe on mielenkiintoinen ja tällä hetkellä myös hyvin ajankohtainen.

Opinnäytetyössä haastavinta oli aiheen rajaamisen ja suurien tietomäärien käsittelyn lisäksi tiedon löytäminen muutamista yksittäisistä aihealueista. Alun perin tarkoituksena oli tehdä opinnäytetyö, jossa käsitellään mobiilin lähimaksamisen tilannetta keskittyen erityisesti NFC-teknologian hyödyntämiseen matkapuhelimella maksettaessa. Työn aihepiiri laajeni hieman, kun NFC-teknologialla huomattiin olevan odotettua laajemmat sovellutusmahdollisuudet. Alun perin oli myös tarkoituksena tarkastella laajemmin Suomen lainsäädännön vaikutuksia mobiilimaksamiseen, mutta aihe oli jo muutenkin venynyt laajaksi ja asian selvittämiseen olisi tarvinnut lisää aikaa.

Käytin tiedonlähteenä internetin suomen- ja englanninkielisiä sivustoja. Varsinkin etämaksamista käsittelevän tiedon löytäminen oli välillä yllättävän hankalaa,

kun taas lähimaksamista ja NFC:tä käsitteleviä lähteitä löytyi yleensä erittäin monipuolisesti. Välillä tietoa ei löytynyt suoraan, mikä lisäsi kirjoittamisen haastavuutta. Opinnäytetyön myötä oma asiantuntemus asiasta on lisääntynyt huomattavan paljon siitä, mitä se oli vielä ennen opinnäytetyön aiheeseen perehtymistä. Tulevaisuudessa on odotettavissa, että tiedot jossakin määrin muuttuvat tämänhetkisestä, mutta asioiden perusperiaatteet eivät todennäköisesti tule muuttumaan merkittävästi. Opinnäytetyön tuloksena aikaansaatu raportti on tarkoitettu kaikkien aiheesta kiinnostuneiden käyttöön.

Lähteet

Aarinen, R. 2006. Miten NFC tekniikka toimii. Aariset Oy. www.aariset.com/RFID/NFC.doc. 9.4.2012.

Advanced Card System Ltd. 2012. ACR122U NFC Contactless Smart Card Reader. http://www.acr122.com/pages/contactless-readers/about. 21.5.2012.

Alkio, J. 2011. Aina osti mobiilimaksamista. Tietoviikko. http://www.tietoviikko.fi/kaikki_uutiset/aina+osti+mobiilimaksamista/a595346. 13.2.2012.

Bank of Montreal. 2012. Tap & Go with MasterCard®* PayPass™*. http://www.bmo.com/home/personal/banking/credit-cards/my-bmo-credit-card/paypass. 18.4.2012.

Baron, K. Oyster card. http://www.flickr.com/photos/kalleboo/3209074959/. 16.4.2012.

Bell, C. 2010. Samsungin puhelin avaa lukot. ITNyt. http://www.itnyt.fi/it-uutiset/1703-samsungin-puhelin-avaa-lukot. 25.4.2012.

Cangeloso, S. RFID tag anything with Tikitag. Geek.com. http://www.geek.com/articles/chips/rfid-tag-anything-with-tikitag-20080930/. 18.4.2012.

Chambers, L. 2011. PayPal Uses NFC to Make Peer-to-Peer Payments Easier than Ever. https://www.thepaypalblog.com/2011/07/paypal-uses-nfc-to-make-peer-to-peer-payments-easier-than-ever/. 18.4.2012.

City of Oulu -project. 2008. Services through NFC technology. ITEA Smart-Touch. Tekes. http://ttuki.vtt.fi/smarttouch/www/kuvat/December08_Newsletter.pdf. 28.2.2012.

Digiraha. 2008. Usein kysyttyjä kysymyksiä. Osuuspankki. http://web.archive.org/web/20080821114013/http://www.digiraha.net/digirahaKysymykset.html#0. 20.4.2012.

DiMauro, J. Tikitag and Field Notes: Hello, World. http://www.flickr.com/photos/jazzmasterson/3317485442/. 17.4.2012.

FiCom ry. 2008. Kontaktiton lähiasiointi matkapuhelimella, eLippu matkapuhelimessa. http://www.ficom.fi/linked/fi/ohjeita/FiCom_eLippu_matkapuhelimessa_1.pdf. 8.5.2012.

Foley, M. 2012. RFID-sirut ja yksityisyys. Your Security Resource. http://www2.yoursecurityresource.com/nortonretail/fi/articles/rfid/index.html#axzz1uwLqrw46. 24.2.2012.

Frilander, A. 2011. Osuuspankin Digiraha kuolee. Tietoviikko. http://www.tietoviikko.fi/kaikki_uutiset/osuuspankin+digiraha+kuolee/a584414. 26.1.2012.

Fujitsu. 2009. Mobiilimaksu on tahdon asia. http://www.net-lehti.com/netlehtiarkisto/net309/www.net-lehti.com/defaultcfbf.html?ContentID=1131. 30.1.2012.

Houbrechts, J. Ping.Ping iPhone. http://www.flickr.com/photos/choubistar/5508445051/. 18.4.2012.

Hämäläinen, M. 2002. Näin toimii UWB tiedonsiirto. Tietokone. http://www.tietokone.fi/lehti/tietokone_6_2002/nain_toimii_uwb_tiedonsiirto_4153. 8.5.2012.

Innopay. 2011. Mobile payments 2012 - My mobile, my wallet? http://www.mobilepay.nu/afbeeldingen/Innopay-Mobile-Payments-2012.pdf. 9.5.2012.

Jyväskylän yliopisto. 2012. Autentikointi(todennus). https://www.jyu.fi/thk/ohjeet/sanasto/autentikointi. 4.4.2012.

Kainulainen, R. 2011. Near Field Communication ja sen tietoturvaongelmat. TWiki. https://jop.cs.tut.fi/twiki/bin/view/Tietoturva/Tutkielmat/NFC-tietoturva. 3.4.2012.

Kalliokoski, P. 2008. Tulevaisuuden kauppaa testataan Oulussa. Technopolis. http://www.hightechforum.fi/index.cfm?o=omakanava&j=732528&okyId=2. 1.3.2012.

Kapanen, H. 2010. Siirtyykö maksukortti puhelimeen? Luottokunta. http://www.suomenpankki.fi/fi/rahoitusjarjestelman_vakaus/km_yhteistyo/Documents/07_Kapanen_Heikki_Luottokunta_Siirtyyko_maksukortti_puhelimeen.pdf. 30.1.2012.

Karinen, V. 2004. Maksuttomia WAP-palveluja? Tietoa wapista ja sen käyttöönotosta. 4mobile. http://www.4mobile.net/wap-gprs.php. 13.2.2012.

Kemiläinen, M. 2012. Wearable Antennas for Smart Clothing. Tampere University of Technology. http://www.tut.fi/en/current/wearable-antennas-for-smart-clothing-p026710c2. 24.4.2012.

Kesko. 2012. Etäluettava K-Plussa-käteiskortti helpottaa kassalla asiointia. http://www.kesko.fi/fi/Media/Tiedotteet/Lehdistotiedotteet/2011/Etaluettava-K-Plussa-kateiskortti-helpottaa-kassalla-asiointia-/. 15.5.2012.

Kolehmainen, A. 2011a. Nokian uusilla nfc-puhelimilla voi myös maksaa. Tietoviikko. http://www.tietoviikko.fi/kaikki_uutiset/nokian+uusilla+nfcpuhelimilla+voi+myos+maksaa/a673531. 4.4.2012.

Kolehmainen, A. 2011b. PayPalin nfc-sirumaksamista voi kokeilla jo Ruotsissa. MikroPC. http://www.mikropc.net/kaikki_uutiset/paypalin+nfcsirumaksamista+voi+kokeilla+jo+ruotsissa/a743990. 30.1.2012.

Kolehmainen, A. 2011c. Nfc-maksaminen tulee parkkimittareihin. Tietoviikko. http://www.tietoviikko.fi/kaikki_uutiset/nfcmaksaminen+tulee+parkkimittareihin/a747737. 1.3.2012.

Kolehmainen, A. 2012. Kuinka kauan kännykkälompakkoa pitää vielä odottaa? MikroPC. http://www.mikropc.net/kaikki_uutiset/kuinka+kauan+kannykkalompakkoa+pitaa+viela+odottaa/a749807. 14.3.2012.

Koskinen, J. 2011. Sähköinen maksaminen. TWiki. https://jop.cs.tut.fi/twiki/bin/view/Tietoturva/S%e4hk%f6inenMaksaminen. 26.1.2012.

Kuluttajavirasto. 2009. Haamuostokset puhelinlaskussa sortavat kuluttajaa. http://www.kuluttajavirasto.fi/fi-FI/060309/. 20.5.2012.

Kurt, T. 13.56 MHz Mifare tag kit from TrossenRobotics. http://www.flickr.com/photos/todbot/449020281/in/photostream/. 26.4.2012.

Lehto, T. 2012. Luottokunta: Nfc-maksukortit lyömässä läpi. 3T. http://www.3t.fi/artikkeli/uutiset/teknologia/luottokunta_nfc_maksukortit_lyomassa_lapi. 3.4.2012.

Leidenius, K. 2007. Kännykkämaksu tulee taas. Tietokone. http://www.tietokone.fi/lehti/tietokone_7_8_2007/kannykkamaksu_tulee_taa_1239. 8.5.2012.

Logimek Oy. 2012. RFID- järjestelmä. http://www.logimek.fi/RFID_system.php. 21.2.2012.

Luottokunta. 2011a. Luottokunnan asiakasviesti, syksy 2011. http://www.luottokunta.fi/portal/page/portal/fi/liitetiedostot/Luottokunta_Info_3.11_Con_netti.pdf. 18.4.2012.

Luottokunta. 2011b. Vuosikertomus 2011. http://vuosikertomus.luottokunta.fi/FI/markkinatrendit.html. 14.5.2012.

Luottokunta. 2012a. Kontaktiton maksaminen. http://www.luottokunta.fi/fi/vastaanottopalvelut/maksujen_vastaanotto/kontaktiton_maksaminen. 30.1.2012.

Luottokunta. 2012b. Matkapuhelimella. http://www.luottokunta.fi/fi/vastaanottopalvelut/maksujen_vastaanotto/kontaktiton_maksaminen/matkapuhelimella. 30.1.2012.

Luottokunta. 2012c. Kortilla. http://www.luottokunta.fi/fi/vastaanottopalvelut/maksujen_vastaanotto/kontaktiton_maksaminen/kortilla. 30.1.2012.

Luottokunta. 2012d. Lähimaksamisen aika alkaa nyt – päivitä päätteesi. http://www.luottokunta.fi/fi/luottokunta/Luottokunta_Info/Valmistaudu_lahimaksamiseen. 6.5.2012.

Luottokunta. 2012e. Luottokunnan asiakasviesti, kevät 2012. http://www.luottokunta.fi/portal/page/portal/fi/liitetiedostot/Luottokunta_Info_1.12_netti.pdf. 9.5.2012.

MasterCard. 2012. Getting Started. http://www.mastercard.com/us/paypass/phonetrial/gettingstarted.html#. 23.4.2012.

Metivier, P. MWC 2012. http://www.flickr.com/photos/feuilllu/6950321721/. 12.4.2012.

Metivier, P. NFC iCarte iPhone. http://www.flickr.com/photos/feuilllu/6350933397/. 12.4.2012.

Mitchell, B. 2012. Bluetooth. About.com. http://compnetworking.about.com/cs/bluetooth/g/bldef_bluetooth.htm. 9.5.2012.

Mobiiliopas. 2012. Mobiililaitteet. AVO-hanke. https://sites.google.com/site/avomobiiliopas/mobiililaitteet. 24.1.2012.

Mobile Payment Forum. 2002. Mobile Payment Forum White Paper. http://web.archive.org/web/20070710091908/http://www.mobilepaymentfo-
fo-
rum.org/documents/Mobile_Payment_Forum_White_Paper_December_2002.pdf. 11.4.2012.

Movila. 2012. Tekstiviestimaksaminen. http://www.movila.fi/palvelut/tekstiviestimaksaminen. 13.2.2012.

NFC Forum. 2012. NFC in Action. http://www.nfc-forum.org/aboutnfc/nfc_in_action/. 14.3.2012.

NFC-työryhmä. 2010. NFC-työryhmän väliraportti. Liikenne- ja viestintäministeriö. http://www.lvm.fi/c/document_library/get_file?folderId=964902&name=DLFE-10966.pdf&title=NFC-tyoryhman_valiraportti. 26.2.2012.

NFC-työryhmä. 2011. Near Field Communications, NFC-työryhmän loppuraportti. Liikenne- ja viestintäministeriö. http://www.lvm.fi/c/document_library/get_file?folderId=1551284&name=DLFE-11779.pdf&title=Julkaisuja%204-2011. 15.3.2012.

Nokia. 2012. Tee elämästä yksinkertaisempaa, helpompaa ja hauskempaa. http://www.nokia.com/fi-fi/tuotteet/belle-nfc-phones/. 3.5.2012.

OP-Pohjola-ryhmä. 2012. Lähiluettavalla kortilla pienet maksut ilman PIN-koodia. https://www.op.fi/op/henkiloasiakkaat/kortit/valitse-sopiva-kortti?cid=151630690&srcpl=4. 2.6.2012.

Paypal. 2012a. PayPal is the faster, safer way to pay and get paid online. https://www.paypal-media.com/about. 30.1.2012.

Paypal. 2012b. Micropayments. https://www.paypalobjects.com/IntegrationCenter/ic_micropayments.html. 30.1.2012.

Pitkänen, M. 2012. OP-Pohjola ottaa käyttöön etäluettavat maksukortit. AfterDawn. http://fin.afterdawn.com/uutiset/artikkeli.cfm/2012/03/21/op-pohjola_ottaa_kayttoon_etaluettavat_maksukortit. 3.4.2012.

Pohjois-Karjalan ammattikorkeakoulu. 2012. Uutta tekniikkaa uudessa kirjastossa. http://www.ncp.fi/index.php/ajankohtaista/index.php?option=com_content&view=article&id=786. 3.4.2012.

Prisma Research Oy. 2006. Mobiilipalvelumarkkinat Suomessa 2005. Liikenne- ja viestintäministeriö. http://www.lvm.fi/fileserver/Julkaisuja%2022_2006.pdf. 11.4.2012.

Radio-Electronics.com. 2012. NDEF, NFC Data Exchange Format. http://www.radio-electronics.com/info/wireless/nfc/nfc-near-field-communications-data-exchange-format-ndef.php. 8.5.2012.

Ray, B. 2011. NFC in a SIM: They might just have done it. The Register. http://www.theregister.co.uk/2011/11/16/nfc_sim_again/. 28.5.2012.

RFID Lab Finland ry. 2012a. Hyödyllisiä termejä. http://www.rfidlab.fi/hy%C3%B6dyllisi%C3%A4-termej%C3%A4. 21.2.2012.

RFID Lab Finland ry. 2012b. RFID-tekniikan käyttämät taajuusalueet. http://www.rfidlab.fi/rfid-tekniikan-k%C3%A4ytt%C3%A4m%C3%A4t-taajuusalueet. 20.2.2012.

RFID Lab Finland ry. 2012c. RFID-tietoutta. http://www.rfidlab.fi/rfid-tietoutta. 2.2.2012.

RFID Lab Finland ry. 2012d. NFC. http://www.rfidlab.fi/nfc. 25.1.2012.

RFID Lab Finland ry. 2012e. Usein kysyttyä. http://www.rfidlab.fi/usein-kysytty%C3%A4. 20.2.2012.

RFID Lab Finland ry. 2012f. RFID-standardit. http://www.rfidlab.fi/rfid-standardit. 27.5.2012.

RFID Lab Finland ry. 2012g. RFID-tekniikan perusteet. http://www.rfidlab.fi/rfid-tekniikan-perusteet. 21.2.2012.

Rinta, N. 2012. Nfc-kännykkää kokeillaan lentokentällä. Tietoviikko. http://www.tietoviikko.fi/kaikki_uutiset/nfckannykkaa+kokeillaan+lentokentalla/a763298?fail=f. 13.3.2012.

Rouse, M. 2005. M-commerce (mobile commerce). SearchMobileComputing. http://searchmobilecomputing.techtarget.com/definition/m-commerce. 13.2.2012.

Rouse, M. 2007. Over the Air (OTA). SearchMobileComputing. http://searchmobilecomputing.techtarget.com/definition/Over-the-Air. 9.5.2012.

Sanastokeskus TSK. 2007. Mikromaksu. http://www.tsk.fi/tsk/termitalkoot/en/node/266?page=get_id&id=ID36&vocabulary_code=TSKTT. 11.5.2012.

Seppä, H. 2009. Etätunnistusteknologian kehitys meillä ja maailmalla. Tekes. www.tekes.fi/fi/document/27018/rfid_pdf.pdf. 20.2.2012.

Seppä, H. 2011. RFID-etätunnistus - mahdollisuudet ja uhat. Eduskunnan tulevaisuusvaliokunta. http://www.eduskunta.fi/triphome/bin/thw.cgi/trip?${APPL}=erekj&${BASE}=erekj&${THWIDS}=0.3/1338303903_98289&${TRIPPIFE}=PDF.pdf. 19.2.2012.

SFS ry. 2012. Standardisointiin liittyviä termejä ja lyhenteitä. http://www.sfs.fi/standardien_laadinta/mita_standardisointi_on/lyhenteet/. 16.5.2012.

Siru Mobile Oy. 2012a. Usein kysytyt kysymykset. http://www.sirumobile.fi/ukk.html. 18.5.2012.

Siru Mobile Oy. 2012b. Turvallisuus. http://www.sirumobile.fi/turvallisuus.html. 18.5.2012.

Siru Mobile Oy. 2012c. Laskuta asiakastasi tekstiviestillä! http://www.sirumobile.fi/sms.html. 13.2.2012.

Smart Card Alliance. 2012. NFC Resources. http://www.smartcardalliance.org/pages/smart-cards-applications-nfc. 15.4.2012.

Suikkanen, J. 2011a. NFC muuttaa joukkoliikenteen maksamista ja informaatiota. Bonwal Oy. http://www.pllry.fi/liitteet/vk2011_esitys_js.pdf. 4.4.2012.

Suikkanen, J. 2011b. Älykortit & NFC puhelimet, monipuolisia palvelumahdollisuuksia. Bonwal Oy. http://nfc2012.vtt.fi/sus/materiaali/%C4lykortti%20NFC%20puhelimen%20kanssa.pdf. 11.4.2012.

Sunsero. 2012. NFC-tunnisteet. http://www.sunsero.fi/nfc_tunnisteet/. 16.4.2012.

TechTerms. 2008. Emulation. http://www.techterms.com/definition/emulation. 19.5.2012.

Tilastokeskus. 2011. Liitetaulukko 7. Matkapuhelimen käyttö internetin selailuun, sähköpostien lukemiseen, paikannus- ja reittipalveluihin ja maksamiseen iän, toiminnan, koulutusasteen, asuinpaikan kaupunkimaisuuden ja sukupuolen mukaan 2011, %-osuus väestöstä. http://www.stat.fi/til/sutivi/2011/sutivi_2011_2011-11-02_tau_007_fi.html. 5.2.2012.

ToP Tunniste Oy. 2012a. NFC-tunnisteet. http://www.toptunniste.fi/index.php?id=nfc-tags. 16.4.2012.

ToP Tunniste Oy. 2012b. NFC-laitteet. http://www.toptunniste.fi/index.php?id=nfc-devices. 23.4.2012.

ToP Tunniste Oy. 2012c. SmartParking. http://www.toptunniste.fi/index.php?id=rfid-parking. 1.3.2012.

Tuominen, T. 2002. Mobiilimaksamisen menetelmät. Liikenne- ja viestintäministeriö. http://www.lvm.fi/fileserver/31_2002.pdf. 31.1.2012.
Tuominen, T. 2003. Mobiili lähimaksaminen -nykykäyttö ja tulevaisuus. Liikenne- ja viestintäministeriö. http://www.lvm.fi/fileserver/22_2003.pdf. 26.1.2012.
Tupalo.com. Nfc rallye. http://www.flickr.com/photos/ninetomorrows/6788344903/. 26.4.2012.
Uimonen, J. 2003. Maksujärjestelmät ja niiden luokittelu. VirtuaaliAMK. http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/maksaminen.html. 31.1.2012.
Urbaani Sanakirja. 2012. Appletti. http://urbaanisanakirja.com/word/appletti/. 4.4.2012.
Viestintävirasto. 2004. Eurooppalainen taajuuksienkäyttösuunnitelma (ERC Report 25) uusittu. http://www.ficora.fi/index/viestintavirasto/asiakastiedotteet/radiotaajuudet/2004/ECA.html. 5.6.2012.
VISI RFID Solutions Oy. 2012. RFID- Teknologia. http://www.visi-rfid.fi/index.php?option=com_content&view=article&id=2:rfid-teknologia&catid=2:palvelut&Itemid=3. 17.2.2012.
VR-Yhtymä Oy. 2011. Lippujen ostopaikat. http://www.vr.fi/fi/index/junaliput/lippujen_ostopaikat.html#alkuun. 30.5.2012.
VTT. 2012. NFC-tunnistus helpottamaan heikkonäköisten ja näkövammaisten arkea. http://www.vtt.fi/news/2012/18012012.jsp. 17.2.2012.
Vänskä, O. 2011. Baarissa nfc-maksaminen kävisi sekunneissa. Tietoviikko. http://www.tietoviikko.fi/kaikki_uutiset/baarissa+nfcmaksaminen+kavisi+sekunneissa/a740019. 28.2.2012.
Vänskä, O. 2012. Kauppajätti ottaa nfc:n käyttöön Ruotsissa. Tietoviikko. http://www.tietoviikko.fi/cio/kauppajatti+ottaa+nfcn+kayttoon+ruotsissa/a766225. 12.3.2012.
Wikipedia. 2012a. Suoritin. http://fi.wikipedia.org/wiki/Suoritin. 8.5.2012.
Wikipedia. 2012b. Salaus. http://fi.wikipedia.org/wiki/Salaus. 4.4.2012.
Wikipedia. 2012c. Modulaatio (elektroniikka). http://fi.wikipedia.org/wiki/Modulaatio_%28elektroniikka%29. 18.5.2012.
Wikipedia. 2012d. Personal digital assistant. http://en.wikipedia.org/wiki/Personal_digital_assistant. 8.5.2012.
Wikipedia. 2012e. WLAN. http://fi.wikipedia.org/wiki/WLAN. 9.5.2012.
Wired-Bit Oy. 2012. SMS-palvelut. http://www.wired.fi/default.aspx/SMS-palvelut. 21.5.2012.