Tommi Hakamäki

RFID-tekniikkaan pohjautuvien kulunvalvontajärjestelmien ja lähimaksukorttien turvallisuus

Opinnäytetyö
Kevät 2015
SeAMK Tekniikka
Tietotekniikan Tutkinto-ohjelma

SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikka

Tutkinto-ohjelma: Tietotekniikka

Suuntautumisvaihtoehto: Sulautetut järjestelmät

Tekijä: Tommi Hakamäki

Työn nimi: RFID-tekniikkaan pohjautuvien kulunvalvontajärjestelmien ja lähimaksukorttien turvallisuus

Ohjaaja: Heikki Palomäki

Vuosi: 2015 Sivumäärä: 68 Liitteiden lukumäärä: 0

RFID-tekniikkaan pohjautuvia kulunvalvontajärjestelmiä ja lähimaksukortteja hyödynnetään laajasti ihmisten päivittäisissä toiminnoissa. Kuitenkin vain harva tietää kuinka tämä tekniikka toimii. Kulunvalvontajärjestelmien varsinaista tietoturvallisuutta ei ole epäilty julkisesti, vaikka laitteille on esitelty useita erilaisia murtotapoja. Lähimaksukorttien käyttöönotto on herättänyt samantapaisia kysymyksiä, mutta sekä kulunvalvontajärjestelmien että lähimaksukorttien tietoturva on saanut vain vähän mediahuomiota.

Tämän opinnäytetyön tarkoituksena on esitellä RFID-tekniikan toimintaperiaatteet, tietoturvatavat sekä erilaiset tavat, joilla RFID-järjestelmiä on murrettu. Lähimaksukorttien tietoturvaa käsitellään myös ja tarkastellaan millä tasolla kyseinen tietoturva on.

Työn lopputuloksissa käsiteltiin RFID-tekniikkaan pohjautuvien kulunvalvontajärjestelmien ja lähimaksukorttien turvallisuuden huonoa tasoa. Lisäksi pohdittiin mahdollisia syitä turvallisuuden nykytilanteeseen.

Avainsanat: RFID, kulunvalvonta, lähimaksu, lähimaksukortit

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Information Technology

Specialisation: Embedded Systems

Author: Tommi Hakamäki

Title of thesis: Information security of RFID-based access control systems and contactless payment cards

Supervisor: Heikki Palomäki

Year: 2015 Number of pages: 68 Number of appendices: 0

RFID-based access control systems and contactless payment cards are used in various applications in people's everyday lives. Nevertheless only few know how this technology actually works. The information security of access control systems has not been discussed in public even though several different hacking methods for the systems have been developed and published. Implementation of contactless payment cards has got similar attention, but media attention has still stayed rather low.

The purpose of this thesis is to present the basics of RFID-technology, the methods of information security and the several different hacking methods that have been published in one form or another. The information security of contactless payment cards will also be covered and the current security status will be assessed.

As a result of this thesis the unsecure state of RFID-based access control systems and contactless payment cards was processed. Also the possible causes for the current situation were considered.

Keywords: RFID, access control, contactless payment, contactless payment cards

SISÄLTÖ

Kuva-, kuvio- ja taulukkoluettelo

Käytetyt termit ja lyhenteet

ABS	Acrylonitrile Butadiene Styrene, eli Akryylinitriilibutadieenistyreeni on yleisesti käytetty kestävä muovilaatu.
APDU	Application Protocol Data Unit on standardoitu kommunikaatiotapa lähimaksukorttin tai maksukorttin ja lukijan välillä.
ASCII	American Standard Code for Information Interchange on 7-bittinen eli 128 merkkipaikan laajuinen tietokoneiden merkistö.
ASK	Amplitude-Shift Keying, eli amplitudimodulaatio on signaalin amplitudin modulointitapa.
Bluetooth	Bluetooth on avoin standardi laitteiden langattomaan kommunikointiin lähietäisyydellä.
DBP	Differential-Bi-Phase on koodaustapa, jossa binääridata koodataan puolen bitin muutoksilla.
EEPROM	Electronically Erasable Programmable Read-Only Memory on haihtumaton puolijohdemuisti, joka voidaan uudelleen kirjoittaa.
EPCglobal	Electronic Product Code global on tuotetunnisteiden käyttöä ja standardisointia edistävä organisaatio.
FSK	Frequency-Shift Keying, eli taajuusmodulaatio on signaalin taajuuden modulointitapa.
Gen 2	Generation 2 on laitteiston tai ohjelmiston toinen sukupolvi.
HF	High Frequency on radiotaajuusalue välillä 3–30 MHz.

IBM	International Business Machines Corporation on yhdysvalloissa perustettu kansainvälinen tietotekniikka- ja konsultointiyhtiö.
IEC	International Electrotechnical Commission on kansainvälinen sähköalan standardointiorganisaatio.
IFF	Identification; Friend or Foe, eli omakonetunniste on radiosignaali, jonka perusteella toiset lentokoneet ja ilmavalvonta tunnistavat lentokoneen.
ISO	International Organization for Standardization on kansainvälinen standardisoimisjärjestö.
LF	Low Frequency on radiotaajuusalue välillä 30–300 kHz.
Lähimaksukortti	NFC-tekniikkaa hyödyntävä kontaktiton maksukortti.
NDEF	NFC Data Exchange Format on NFC Forumin tukemien laitteiden tiedonsiirtorakenne.
NFC Forum	Near Field Communication Forum on Nokian, Phillipsin ja Sonyn perustama NFC:n standardointia, kehitystä ja käyttöönottoa edistävä organisaatio.
NFC	Near Field Communication on RFID-tekniikkaa hyödyntävä tapa laitteiden tunnistukseen ja tiedonsiirtoon hyvin lyhyille etäisyyksille.
NRZ	Non-Return-to-Zero on koodaustapa, jossa ei palata missään vaiheessa perustilaan.
OOK	On/Off Keying, eli päälle/poismodulaatio on signaalin lähetyksen keskeytystä hyödyntävä modulointitapa.
PIN	Personal Identification Number, eli tunnusluku on salasanana käytettävä luku, jolla voidaan tunnistautua järjestelmään.

PPC	Pulse-Pause Coding on datan koodaustapa lukijalta tunnisteelle, jossa binääridata koodataan lyhyillä pulsseilla.
PSK	Phase-Shift Keying, eli vaihemodulaatio on signaalin vaiheen modulointitapa.
RFID	Radio Frequency IDentification, eli radiotaajuinen etätunnistus on menetelmä tiedon etälukuun ja -tallentamiseen käyttäen RFID-tunnisteita.
ROM	Read Only Memory on mikroprosessoria käyttävän laitteen pysyväismuisti, johon ei voi tehdä muutoksia normaalikäytön aikana.
SIM	Subscriber Identity Module on älykortti, jota käytetään pääsääntöisesti matkapuhelinliittymän tilaajan yksilöllisen asiakasavaimen tietoturvalliseen tallentamiseen.
SNDEF	Short NFC Data Exchange Format on NDEF:n pohjautuva lyhennetty tiedonsiirtorakenne.
UHF	Ultra High Frequency on radiotaajuusalue välillä 0,3–3 GHz.

1 JOHDANTO

1.1 Työn tausta

RFID-tekniikkaan pohjautuvien kulunvalvontajärjestelmien ja lähimaksukorttien näkyvä hyödyntäminen on lisääntynyt näkyvästi viimeisen vuosikymmenen aikana. Kulunvalvontajärjestelmien hyödyntäminen on yleistynyt oppilaitoksissa, kaupoissa, yrityksissä ja julkishallinnon kohteissa, kuten sairaaloissa, terveyskeskuksissa, poliisi- ja paloasemissa. Useissa etälukujärjestelmien kohteissa RFID-tekniikkaa hyödyntämällä välitetään yksityistä tai yleisen turvallisuuden kannalta tärkeää tietoa. Arkaluonteista ja yksityistä tietoa voivat olla esimerkiksi kulunvalvontajärjestelmien tunnistekoodit suojattuihin kohteisiin tai maksukorteilta löytyvät kortti- ja käyttäjätiedot. Logistiikan tarpeisiin pohjautuvaa RFID-tekniikkaa hyödynnetään erilaisissa turvalaitesovelluksissa, paikallisliikenteen matkakorteissa, e-passeissa, lähimaksukorteissa sekä monissa muissa erilaisissa sovelluksissa. Erityistä huomiota ovat saaneet edellä mainitut lähimaksukortit, joilla pyritään tarjoamaan uudempi, nopeampi ja ennen kaikkea turvallisempi tapa suorittaa päivittäisiä ostoksia ja hankintoja.

RFID-tekniikan hyödyntäminen passeissa ja erilaisissa maksukorteissa on herättänyt kuluttajissa mielenkiintoa RFID-tekniikan tietoturvaa kohtaan. Laitteistojen valmistajat ja palveluiden tarjoajat ovat vakuutelleet laitteistojen turvallisuutta ja luotettavuutta. Vuonna 2011 Suomen Eduskunnan tulevaisuusvaliokunnan julkaisussa todetaan, että kulunvalvonnassa käytettyjä RFID-tunnisteita ei ole pystytty kopioimaan. Julkaisussa todettiin myös kuinka hämmästyttävän vähäistä tunnisteiden väärinkäyttö on verrattuna siihen, kuinka paljon tunnisteita on jo käytetty. (Seppä 2011.)

Vuoteen 2011 mennessä oli kuitenkin jo esitelty useita eri tapoja erilaisten RFID-tekniikkaan pohjautuvien tunnisteiden luvattomaan kopiointiin ja hyödyntämiseen. Tästä voidaan päätellä, että RFID-tekniikan yleistyessä ja kasvaessa erilaiset organisaatiot aina valtiollisista kaupallisiin eivät aina ole selvillä mikä on tietyn tekniikan tai laitteiston todellinen tietoturva. Tieto RFID-tekniikan tietoturvaongelmista ei myöskään aina saavu kuluttajien tietoisuuteen ja ainoaksi tiedontarjoajaksi jäävät

laitteistoja myyvät tai hyödyntävät osapuolet. Tästä johtuen tietoturvaongelmia käsittelevä tieto muuttuu huomattavasti riippuen lähteestä ja on usein puutteellista, joten on tärkeää pystyä muodostamaan yhtenäinen ja kattava kuvaus erilaisten käytössä olevien RFID-järjestelmien todellisesta tietoturvasta ja mahdollisista riskeistä.

RFID-kulunvalvontajärjestelmien ja lähimaksukorttien tietoturva koostuu samoista osista kuin klassinen tietoturva, lisäksi pyritään määritelmää laajentamalla käsittelemään erikoistuvat osiot. Klassinen tiedon arvoon perustuva määritelmä koostuu tiedon luottamuksellisuudesta, käytettävyydestä ja eheydestä. Tämä ei kuitenkaan vastaa kaikkia nykyaikaisia vaatimuksia. Laajennetulla tietoturvallisuuden määritelmällä pyritään ottamaan huomioon tiedon tuottaja ja omistajan identiteetti, samalla pyritään kohottamaan laitteistojen ja tieto- ja tietoliikennejärjestelmien arvoa. Oletusarvoisesti pyritään turvaamaan arkaluonteinen ja yksityinen tieto. (Hakala, Vainio, Vuorinen, 2006, 4-6.)

1.2 Työn tavoite

Tämän opinnäytetyön tavoitteena on tuottaa kattava selvitys RFID-kulunvalvontajärjestelmien ja lähimaksukorttien tietoturvasta ja mahdollisista riskeistä. Lisäksi tavoitteena on, että opinnäytetyötä voidaan käyttää hyväksi RFID-tekniikan perusteiden ja sen tietoturvan selvittämisessä kuluttajille ja henkilöille jotka eivät omaa soveltavan alan koulutusta tai kokemusta.

Tavoitteena on selvittää vastaus kysymykseen RFID-tekniikan tietoturvallisuudesta ja selvittää mihin kolmesta loppupäätelmästä opinnäytetyön tutkimustuloksena saavutaan. Kolme todennäköistä loppupäätelmää ovat:

1. Tietoturva on hyvä ja tekniikkaa voidaan hyödyntää turvallisesti ja ilman riskejä
2. Tietoturva on huono ja tekniikan hyödyntämisessä on riskejä
3. Tietoturva on huono, mutta tilastolliset todennäköisyydet ja sekundaariset turvaominaisuudet ehkäisevät riskien syntymistä

Tässä opinnäytetyössä hyödynnetään tutkimusmenetelmänä tiedon hakemista ja käsittelemistä asiaan perehtyneistä julkaisuista ja sivustoista. Kaiken kerätyn tiedon suhteen on pyritty toimimaan erittäin lähdekriittisesti, arvioimaan kirjoittajan tai julkaisijan lähtökohtia ja mahdollisuuksien mukaan varmentamaan saadut tiedot useammasta lähteestä.

1.3 Työn rakenne

Opinnäytetyö rakentuu neljästä pääosuudesta, joilla on jokaisella oma lähtökohtansa ja tavoitteensa. Pääkohdat ovat järjestyksessä johdanto, toiminta, tietoturva ja loppupäätelmät. Kaikki neljä osuutta aloitetaan perusteiden läpikäynnillä ja selvittämisellä, josta siirrytään aiheen soveltamiseen yleisemmällä tasolla. Mahdollisuuksien mukaan pyritään myös käsittelemään soveltamista yksityiskohtaisemmissa kohteissa.

Ensimmäisessä osuudessa, johdannossa, esitellään opinnäytetyön lähtökohtia, tavoitteita ja rakennetta, sekä kerrotaan lyhyesti RFID-tekniikan historiasta. Samalla käydään yksinkertaisilla termeillä ja käsitteillä läpi RFID:n, NCF:n ja lähimaksukorttien yksikertainen toiminta. Lisäksi pyritään myös esittämään RFID, NCF ja lähimaksukortit siinä muodossa, että näiden eroavaisuudet ovat selvät.

Toisessa osuudessa, toiminnassa, käsitellään RFID-teknologian ja lähimaksukorttien standardointiin vaikuttavia yhteisöjä, sekä esitellään RFID-järjestelmän eri osat ja niiden toiminta. Lähimaksukortit luetaan kuuluvan RFID-järjestelmään, joten niitä ei käsitellä erikseen.

Kolmannessa osuudessa, tietoturvassa, käsitellään RFID-järjestelmien ja lähimaksukorttien olemassa olevaa tietoturvaa sekä esitellään esimerkkien kautta millaisin eri tavoin ja laittein järjestelmän tietoturva on murrettu.

Neljännessä ja viimeisessä osuudessa, loppupäätelmissä, käsitellään RFID-tekniikan ja lähimaksukorttien tietoturvan tilaa ottaen huomioon edellisissä osuuksissa esitellyt tietoturvan suojaus- ja murtotavat. Käsittelyn aiheina ovat myös olemassa olevien laitteistojen tietoturvan parantaminen ja markkinoinnin vaikutus tietoturvaongelmien ymmärtämiseen.

1.4 RFID-tekniikan historia

RFID-tekniikkaa hyödyntävät etätunnistustekniikat ja lähimaksukortit pohjautuvat teknologialtaan sotilaskäyttöön suunniteltuihin ensiö- ja toisiotutkan keksimiseen. Ensiö- ja toisiotutka taas puolestaan pohjautuvat useiden vaiheiden kautta sähkömagneettisen säteily teoreettiseen tutkimukseen.

Sähkömagneettisten säteilyn tutkimus alkoi vuonna 1864 James Clerk Maxwellin kehittämien yhtälöiden kautta. Kyseisillä Maxwell-yhtälöillä todistettiin sähkömagneettisten säteilyn olemassa olo, mutta vain teoreettisesti. 24 vuotta myöhemmin, vuonna 1888, Heinrich Rudolf Hertz onnistui kehittämään ja rakentamaan prototyyppilaitteiston ja todistamaan sähkömagneettisen säteilyn käytännössä. Hertzin rakentama laitteisto pystyi lähettämään ja vastaanottamaan sähkömagneettista säteilyä mikroaaltotaajuudella. Myöhemmin kansainvälisen yksikköjärjestelmän mukainen taajuuden yksikkö nimettiin Hertzin mukaan. (Miles, Sarma & Williams, 2008, 4-5.)

Sähkömagneettisesta säteilystä alettiin käyttää myös nimitystä radioaalto, joka myöhemmin vakiinnutti asemansa käsitteenä. Hertzin tutkimusten ja prototyyppien kautta kehitettiin ensimmäiset ensiötutkat. Ensiötutka koostuu radiolähettimestä, jonka lähettämistä radioaalloista ja kohteesta heijastuneista radioaalloista voidaan matemaattisesti laskea kohteen etäisyys ja etenemissuunta. Ensiötutka esiteltiin jo 1900-luvun alussa, mutta laitteen tarpeellisuutta ei vieläkään nähty. Vuonna 1912 tapahtuneen valtamerilaiva Titanicin suuronnettomuuden jälkeen huomattiin ensiötutkan tarpeellisuus meriliikenteessä ja -pelastuksessa. (Shepard, 2004, 42-44.)

Toisen maailmansodan uhka ja lentokoneiden korostunut hyödyntäminen sotatoimissa teki tutkan kehityksen ja käyttöönoton mahdolliseksi. Toisen maailman sodan alkaessa vuonna 1939 Yhdysvallat, Iso-Britannia, Saksa, Ranska, Neuvostoliitto, Italia ja Japani olivat onnistuneesti kehittäneet, ja suurin osa ottanut käyttöön, toimivan tutkajärjestelmän. Kyseisiä tutkajärjestelmiä hyödynnettiin lentokoneiden lisäksi sotalaivojen paikannuksessa. (Shepard, 2004, 42-44.)

Ensiötutkajärjestelmässä havaittiin ongelmaksi omien ja vihollisten lentokoneiden ja laivojen erottaminen toisistaan. Vastaukseksi kehitettiin toisiotutka, jonka olen-

naisena osana toimii IFF-tunnistejärjestelmä. IFF-tunnistejärjestelmä koostuu maa-asemasta ja sotakoneisiin asennettavasta toisiotutkavastaajasta. Maa-asema lähettää keskeyttämättä tietyllä radiotaajuudella kyselypulsseja, joihin toisiotutkavastaaja, tai transponderi, lähettää vastauksena oman transponderikoodinsa. Transponderikoodista saadaan selville yksittäiselle lentokoneelle tai laivalle yksilöllinen tunniste. Toisiotutkajärjestelmä oli ensimmäinen esimerkki modernista RFID-järjestelmästä. (Shepard, 2004, 45-47.)

Modernien passiivisten RFID-tunnisteiden edeltäjä oli 1950- ja 1960-luvulla kehitetty ja käyttöönotettu EAS-varkaudenestojärjestelmä, jota hyödynnetään yhä kaupoissa. Tuotteisiin kiinnitettävässä tunnisteessa oli vain yhden bitin muisti, jolla voitiin esittää vain kaksi tilaa: päällä tai sammutettu. Asiakkaan ostettua tuote kytkettiin tunniste sammutettuun tilaan. (Roberti 2005.)

Ensimmäisen modernin RFID-järjestelmän patentti hyväksyttiin vuonna 1967. Kyseinen järjestelmä ei kuitenkaan moderneista RFID-järjestelmistä poiketen hyödyntänyt digitaalista vaan analogista muistia. (Davis, 2009.)

Vuonna 1973 patentoitiin Mario Cardullon toimesta ensimmäinen digitaalista muistia hyödyntävä aktiivitunniste. Samana vuonna Charles Walton patentoi ensimmäisen passiiviseen tunnisteeseen pohjautuvan RFID-järjestelmän. (Shepard, 2004, 49-51.)

Yhdysvaltojen hallituksen kehitysprojektien kautta luotiin pohja yhä käytössä oleville järjestelmille. Los Alamosin Kansallisessa Laboratoriossa kehitettiin 1970-luvulla mikroaaltotaajuuksia käyttäviä RFID-järjestelmiä ydinmateriaalin kuljetuksen valvontaan sekä maatalouden karjaeläinten seurantaan. Ydinmateriaalin kuljetuksen valvonnassa hyödynnettiin aktiivisia transpondereita ja karjaeläinten seurantaan kehitettiin passiivinen RFID-järjestelmä, joka sai toimintavirtansa radioaalloista. Myöhemmin eri yritykset kehittivät matalia taajuuksia käyttäviä järjestelmiä, joissa hyödynnettiin huomattavasti pienempiä transpondereita kuin ennen. Transpondereiden pienentyessä tunniste voitiin esimerkiksi koteloida lasiin ja istuttaa karjaeläinten ihon alle. Pienet tunnisteet mahdollistivat myös tunnisteiden paremman hyödyntämisen sekä logistiikka- että kulunvalvontajärjestelmissä. (Roberti 2005.)

1990-luvun alussa IBM:n insinöörit kehittivät ja patentoivat 0.3–3 GHz;n mikroaaltotaajuutta käyttävän RFID-järjestelmän. Korkeamman taajuuden käyttö mahdollisti suuremman lukuetäisyyden ja tiedonsiirtonopeuden. Alkuvaikeuksien jälkeen vuonna 1999 järjestelmä sai vihdoin suosiota, kun Uniform Code Council, EAN International, Procter & Gamble ja Gilette rahoittivat ja perustivat yhdessä Auto-ID Centerin. Auto-ID:n tarkoituksena oli mahdollistaa halpojen korkeataajuustunnisteiden käyttämisen tuotteissa ja seurata niiden etenemistä toimitusketjussa. (Roberti 2005.)

Vuosien 1999 ja 2003 välillä Auto-ID Center keräsi yli 100 suuren yhtiön tuen, kehitti kaksi tiedonsiirtoprotokollaa, EPC-numerointijärjestelmän ja internetiä hyödyntävän datarakenteen, joiden pohjalta perustettiin EPCglobal. Vuonna 2003 Auto-ID Centerin korvasi Auto-ID Lab. (Roberti 2005.)

1.5 Yksinkertainen toiminnankuvaus

Tässä osiossa käsitellään RFID-laitteiden ja järjestelmien kokoonpano suppeasti ja alustetaan myöhempää, syvempää aiheen käsittelyä.

RFID-laitteistokokonaisuus koostuu aina vähintäänkin kolmesta erillisestä osasta. Nämä osat ovat RFID-tunniste, -lukija ja -hallintajärjestelmä. Laitteistokokonaisuuden näkyvimmät osat ovat tunniste ja lukija. Normaalisti lukija tai lukijat on yhdistetty hallintajärjestelmään, josta voidaan tarkastella ja asettaa sallittuja tunnisteita. (Finkenzeller, 2003, 6-9.) Kokonaisuuden eri osat käydään yksityiskohtaisesti läpi opinnäytetyön tunniste-osuudessa.

Lukijan ja tunnisteen välinen tiedonsiirto tapahtuu LF- ja HF-taajuusalueilla induktiivisen kytkennän, oskilloivan magneettikentän kautta sekä UHF ja mikroaaltotaajuusalueilla varsinaisen radioaaltoja hyödyntävän tiedonsiirtotavan mukaan. Käyttötaajuudesta tai kytkentätavasta riippumatta RFID-tekniikassa hyödynnetään sähkömagneettista säteilyä sen eri muodoissa, erityisesti tunnisteissa joissa ei ole omaa virtalähdettä, vaan toimintavirta otetaan suoraan sähkömagneettisesta säteilystä. (Finkenzeller, 2003, 22-26.)

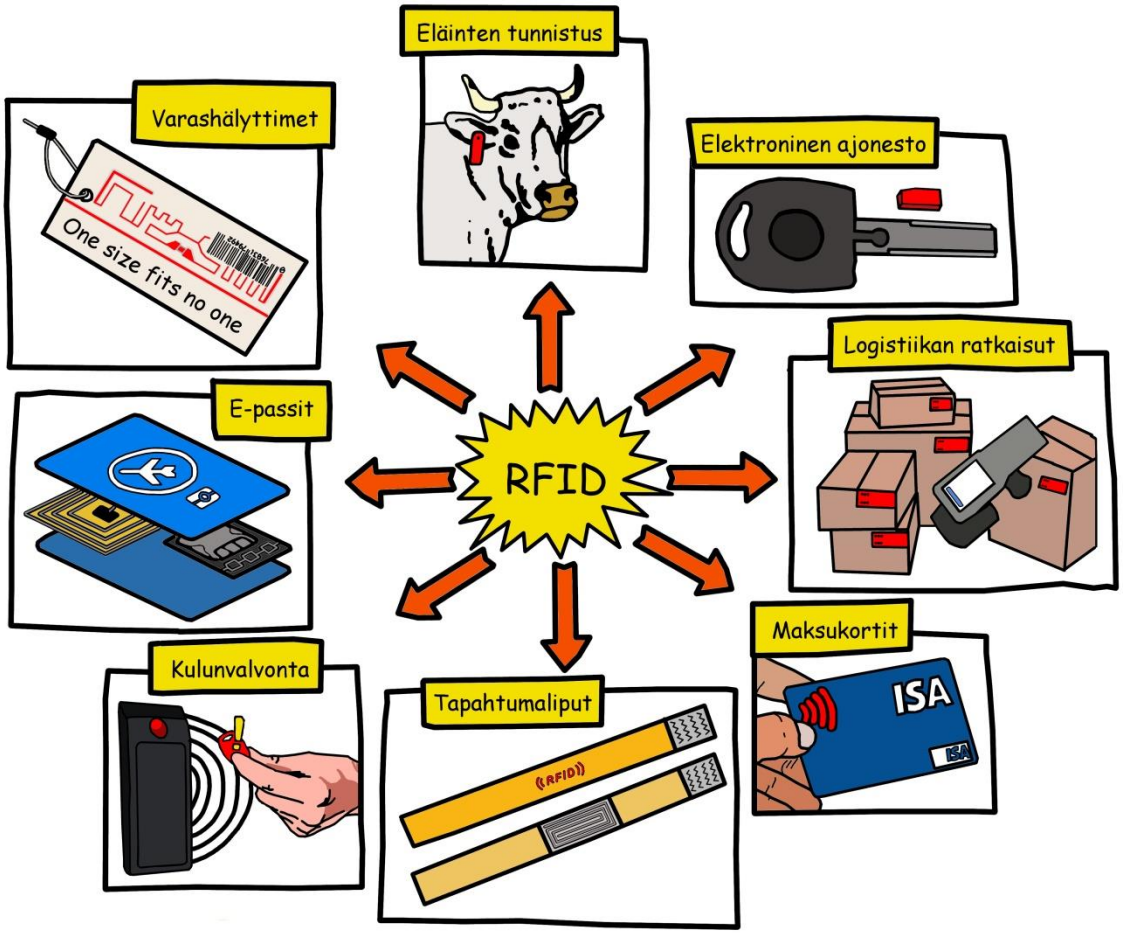
Induktiivista kytkentää tai radioaaltoja moduloimalla, ajastamalla tai muutoin muuntamalla vastaanotetaan ja lähetetään dataa tunnisteen ja lukijan välillä. Hyödynnettävät käyttötaajuudet ovat teoriassa rajattomat, mutta standardoinnin ja yhdenmukaistetun tuotannon johdosta yleisimmässä käytössä olevat taajuusalueet ovat LF, HF ja UHF. Näillä taajuusalueilla on tarkemmin määritellyt taajuudet. Maakohtaisia variaatioita on olemassa, mutta kansainvälisten standardointien avulla pyritään luomaan maailmanlaajuisesti yhtenäisempi taajuusalueiden hyödyntäminen. (Finkenzeller, 2003, 22-26.) Taulukosta 1 voidaan nähdä taajuusalueet ja niiden tarkemmin määritellyt käyttötaajuudet ja kuviosta 1 voidaan nähdä esimerkki yksinkertaistetusta lukutapahtumasta.

Taulukko 1. Käytetyt RFID-taajuudet (CNRFID [Viitattu 24.3. 2015].)

Taajuusalueet	**Termi**	**Käyttötaajuudet**
30–300 kHz	LF (Low Frequency)	125–134,2 kHz
3–30 MHz	HF (High Freqency)	13.56 MHz
300–3000 Mhz	UHF (Ultra High Freqency)	860–960 MHz 2.45 GHz

Kuvio 1. Yksinkertaistettu lukutapahtuma

RFID-tekniikkaa on hyödynnetty maailmalaajuisesti jo lähes vuosisadan ajan ja käyttökohteita on erittäin paljon. Normaalille kuluttajalle tekniikka saattaa olla uutta ja kehittynyttä, mutta todellisuudessa kyse on jo vanhentuvasta teknologiasta, jolle etsitään jatkuvasti uusia käyttökohteita ja sovelluksia. (Violino 2005.) Kuviosta 2. voidaan nähdä erilaisia RFID-tekniikan käyttökohteita.



Kuvio 2. Esimerkkejä RFID-tekniikan käyttökohteista

Tässä opinnäytetyössä käsitellään myös NFC-teknologian sovelluksia. NFC pohjautuu oleellisesti RFID-tekniikkaan, mutta on tärkeää pystyä erottelemaan tekniikat toisistaan. Tekniikoiden erot pohjautuvat tiedonsiirtoon ja käyttötaajuuteen. Suurin osa NFC-sovelluksista on integroitu erilaisiin mobiililaitteisiin tai maksukortteihin, jolloin NFC-piiri voi olla yhdistettynä esimerkiksi SIM-korttiin. (Poole [Viitattu 24.3.2015]).

2 TOIMINTA

Tässä osuudessa esitellään RFID- ja NFC-järjestelmiä koskevat standardisoinnit sekä järjestelmän eri osat. Järjestelmiä määrittelevät standardisoinnit käsitellään vain pääpiirteiltään, mutta tunnisteet, lukijat ja hallintajärjestelmä käsitellään tarkasti laitteiden elektroniikasta aina toimintoihin asti. RFID- ja NFC-järjestelmien tarkempi tiedonsiirto ja erilaiset datarakenteet käsitellään erikseen.

2.1 Standardit

RFID-tekniikan monimuotoisuus mahdollistaa melkeinpä rajattoman määrän erilaisia laite- ja järjestelmäkokonaisuuksia. Muuttuvina tekijöinä tekniikassa ovat muun muassa käyttötaajuus, erilaiset komponentit sekä tiedonsiirto- ja tallennusprotokollat. Tekniikan monimuotoisuus tarjoaa suuren valinnanvapauden erilaisten järjestelmien koostamiseen tarjoten siten useita positiivisia tekijöitä, mutta yleisesti tärkeämmäksi nähdään erilaisten RFID-järjestelmien tuomien samojen standardimääritysten piiriin. Standardoinin tarkoitus RFID-tekniikassa on yhdenmukaistaa järjestelmiä asettamalla niille tarkasti määriteltyjä ehtoja ja vaatimuksia. Standardoinnin avulla voidaan esimerkiksi eri tuottajien laitteita käyttää yhdessä niiden ollessa keskenään yhdenmukaisia. RFID-tekniikan standardointi ei ole kokonaisuudessaan vielä valmis. Tällä hetkellä ainoa täysin valmis standardi on EPCglobal UHF Gen2 V1 -standardia, joka koskee UHF-taajuusalueella toimivia passiivisia RFID-järjestelmiä eli UHF RFID -tunnisteita ja lukijoita. (Impinj [Viitattu 25.3.2015]).

Tärkeimpinä tahoina RFID-tekniikan standardoinnissa toimivat ISO, IEC ja EPCglobal. RFID-tekniikasta johdettavassa NFC-tekniikassa ja sen sovelluksissa hyödynnetään myös ISO- ja IEC-standardeja, mutta lisäksi standardointia ajaa eteenpäin laitevalmistajien Nokia, Sony ja Phillips vuonna 2004 perustama NFC Forum. (Impinj [Viitattu 25.3.2015]). Tässä opinnäytetyössä käsitellään lisäksi lähimaksukortteja, joiden toiminnassa hyödynnetään kaikkien muiden standardien lisäksi vielä EMV-standardia, joka koskee korttimaksujen varmentamista ja teknisiä vaatimuksia.

ISO-, IEC- ja EPCglobal-standardeilla käsitellään RFID-tekniikan hyödyntämistä pääpiirteittäin käyttökohdesovellusten ja ominaisuuksien mukaan. Historiallisesti kyseisillä standardeilla on vaikutettu eläinten tunnistuksessa ja logistiikan tehtävissä käytettävien laitteiden suunnitteluun ja valmistukseen. Samoja standardeja kuitenkin hyödynnetään standardien määrittämättömissä käyttökohteissa, esimerkiksi eläinten tunnistukseen suunniteltuja standardeja hyödynnetään moderneissa kulunvalvonnan sovelluksissa standardin alkuperäisessä muodossa. (Finkenzeller, 2003, 229.)

Taulukko 2. Esimerkkejä ISO-standardeista (Finkenzeller 2003)

Standardi	Määrittelee
ISO 11784 ISO 11785 ISO 14223	Eläinten tunnistuksessa käytettävien tunnisteiden datasisällön, tiedonsiirron ja ilmarajapinnan
ISO 10536	4.9152 MHz:n taajuudella ja alle 1 cm:n lukuetäisyydellä toimivat tunnisteet
ISO 14443	0–10 cm lukuetäisyydellä toimivat tunnisteet
ISO 15693	13.56 MHz:n taajuudella ja 0–1 m:n lukuetäisyydellä toimivat tunnisteet
ISO 18000	Eri taajuudella toimivien tunnisteiden ilmarajapinnan ja pakolliset komennot

NFC Forum pyrkii edistämään NFC-tekniikan käyttöönottoa luomalla erilaisia standardointimalleja ja määrityksiä varmistaakseen laitteiden yhteensopivuuden ja maailmanlaajuiset käyttöympäristöt. ISO- ja IEC-standardeilla on määritelty NFC-

tekniikan niin sanotut pohjamääritykset ja NFC Forum pyrkii niiden pohjalta kehittämään NFC-standardointia. (NFC Forum [Viitattu 25.3.2015.)

EMV-standardoinnilla määritellään integroidun mikropiirin omaavien maksukorttien ominaisuuksia. Standardit käsittelevät muun muassa tiedonsiirtoprotokollaa, yleistä arkkitehtuuria ja tietoturvaa. EMV Contactless -määrityksissä käsitellään kontaktittomien maksukorttien eli lähimaksukorttien ominaisuuksia ja vaatimuksia. Aluksi määriteltiin vain maksuterminaalien vaatimukset, mutta myöhemmin määritykset lisättiin kattamaan kaikki maksutapahtumassa käytettävät laitteet. (EMVCo [Viitattu 25.3.2015].) Kuviosta 3 voidaan nähdä esimerkki lähimaksukortin maksutapahtumasta.

Kuvio 3. Lähimaksutapahtuma

2.2 Tunniste

Tunniste on RFID- tai NFC-järjestelmän käyttäjälle kuuluva osa. Kulunvalvonnan tarkoitukseen suunnitellussa järjestelmässä käyttäjänä toimii henkilö, kun taas lo-

gistiikan käyttöön suunnatussa järjestelmässä tunniste on kiinnitettynä tuotteeseen tai pakettiin. Tunnisteen järjestelmäkohtainen tehtävä on jokaisessa käyttökohteessa silti sama eli toimia kohteen tunnistuksessa hyödynnettävänä laitteena. Käyttökohteita tunnisteille on erittäin paljon ja voidaan hyvin olettaa, että modernissa toimintaympäristössä suurin osa ihmisistä kuljettaa mukanaan jonkin tyyppistä RFID-tekniikkaan pohjautuvaa tunnistetta. (Shepard, 2004, 50-61.)

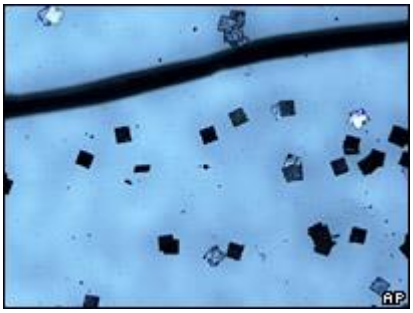
Tunniste koostuu aina vähintäänkin antennista, mikroprosessorista sekä toiminnalle välttämättömistä elektronisista komponenteista. Tunnisteessa voidaan käyttötarkoituksesta ja tyypistä riippuen hyödyntää lisäksi erilaisia ylimääräisiä mikroprosessoreita, sisäisiä virtalähteitä, antureita sekä erilaisia vastuksia ja kondensaattoreita. (Shepard, 2004, 57-74.)

Tunnisteet voidaan jakaa ominaisuuksiensa mukaan passiivisiin, puolipassiivisiin ja aktiivisiin tunnisteisiin. Tunnisteiden erilaiset ominaisuudet vaikuttavat erityisesti toimintaetäisyyksiin.

Passiiviset RFID- tai NFC-tunnisteet ovat kaikkein yleisimpiä ja niitä on saatavilla monessa eri muodossa ja edulliseen hintaan. Kyseiset tunnisteet saavat toimintavirtansa suoraan RFID- tai NFC-lukijalta eivätkä sisällä sisäistä virtalähdettä. Sisäisen virtalähteen puuttuminen vaikuttaa myös tunnisteen tietoturva- ja toiminta-ominaisuuksien vähenemisen. Passiivinen virtaominaisuus vaikuttaa huomattavasti myös tunnisteen lukuetäisyyteen, jolloin yleisin lukuetäisyys on vain useita senttimetrejä. Passiivisten tunnisteiden lukemiseen vaikuttaa kuitenkin enemmän itse lukija kuin tunniste, jolloin erilaisilla lukijoilla voidaan päästä helposti yli 10 metrin etäisyyksiin, joissain tapauksissa voidaan saavuttaa yli 100 metrin lukuetäisyys. (Bonsor, Fenlon 2007.) Kuviossa 4 voidaan nähdä HID Global -valmistajan yleisin passiivinen tunniste.

Kuvio 4. HID Indala Flexkey passiivinen tunniste (HID Global [Viitattu 26.3.2015])

Passiivisten RFID-tunnisteiden vähäisistä komponenttivaatimuksista johtuen on niiden kokoa onnistuttu vuosien varrella pienentämään huomattavasti. Yksi pienimmistä markkinoilla olevista RFID-tunnisteista on sekä leveydeltään että pituudeltaan vain 0,05 millimetriä. Tunnisteen valmistaja Hitachi julkisti tunnisteen vuonna 2007. (BBC 2007.) Kuviosta 5 voidaan nähdä Hitachin tunnisteen koko.



Kuvio 5. Hitachin RFID-tunnisteiden koko hiukseen verrattuna (BBC 2007)

Puolipassiiviset tunnisteet sisältävät passiivisista tunnisteista poiketen sisäisen virtalähteen, jota hyödynnetään oletusarvoisesti vain mikroprosessorin toiminnassa. Virtalähteen avulla mikroprosessori pystyy suorittamaan enemmän toimintoja ja tarjoamaan esimerkiksi nopeamman tiedonkäsittelyn ja turvallisemman salauksen. Puolipassiivisen tunnisteen virtalähdettä ei kuitenkaan hyödynnetä tunnisteen lähetystoiminnoissa, vaan ainoastaan sisäisessä tiedonkäsittelyssä. (CISCO Systems 2008.)

Puolipassiiviseen tunnisteeseen voidaan liittää erilaisia sensoreita ja antureita, jotka tallentavat jatkuvasti tai hetkittäin tietoa tunnisteesta tai tunnisteen ympäristöstä. Logistiikan lämpöherkkien tuotteiden kuljetuksessa voidaan puolipassiivisessa tunnisteessa käyttää lämpötila-anturia, joka pystyy lukuhetkellä lähettämään tiedon kokemistaan lämpötilavaihteluista. (Miles, Sarma & Williams, 2008, 44-46.) Kuviosta 6 voidaan nähdä esimerkki puolipassiivisesta tunnisteesta, johon on liitetty anturi.

Kuvio 6. CEAN RFID:n valmistama puolipassiivinen tunniste lämpötila- ja kosteusanturilla (Cadamuro 2011)

Aktiivinen tunniste on kolmesta tunnistetyypistä ominaisuuksiltaan kattavin. Passiiviseen ja puolipassiiviseen verrattuna voidaan aktiiviselle tunnisteelle tallentaa huomattavasti suurempia tietomääriä, sen lukuetäisyys ei riipu ainoastaan lukijasta, ja siihen voidaan puolipassiivisen tunnisteen tapaan liittää erilaisia sensoreita ja antureita. Aktiivinen tunniste sisältää sisäisen virtalähteen ja oman lähetinpiirin, joiden avulla lukuetäisyydestä on saatu mahdollisimman suuri. (Poole [Viitattu 24.3.2015].)

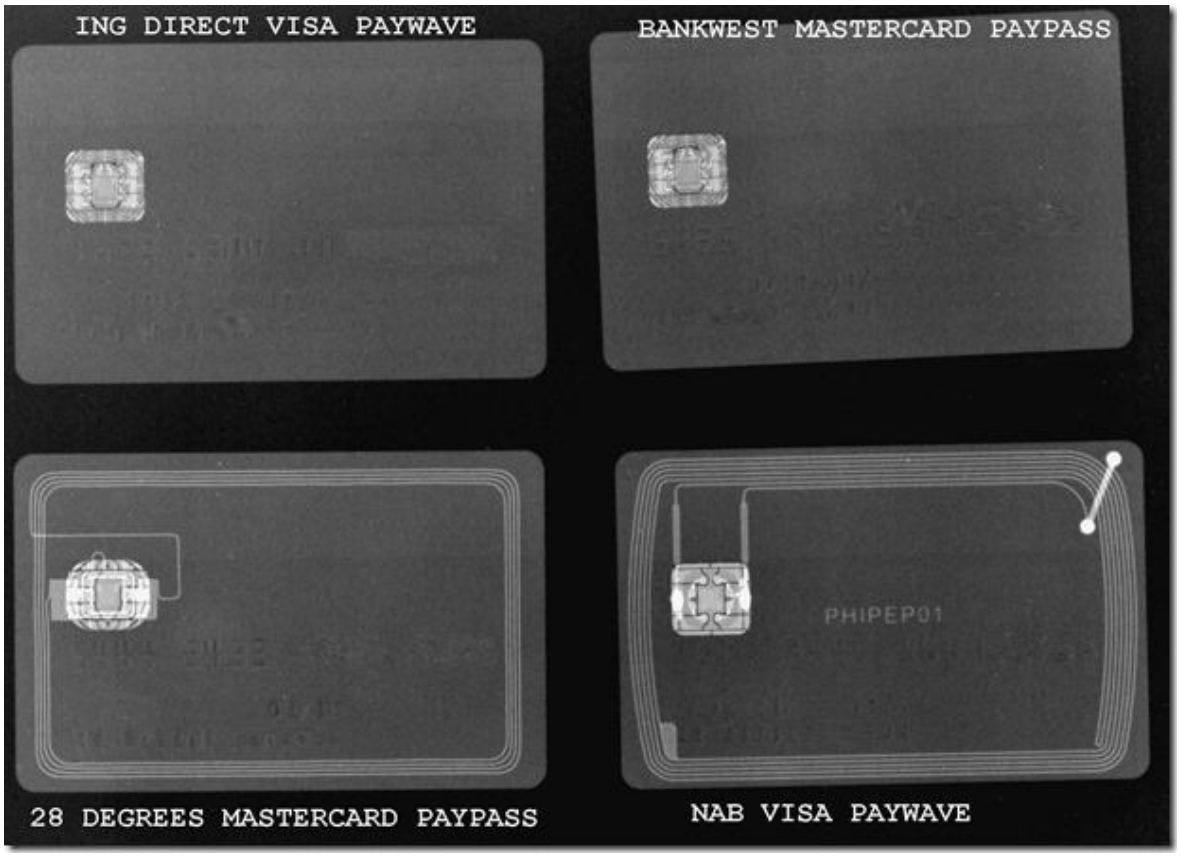
Aktiivisia tunnisteita voidaan hyödyntää esimerkiksi tietyllä alueella tapahtuvassa reaali-aikaisessa tunnisteen seurannassa. 2,4 GHz:n käyttötaajuutta hyödyntäviä aktiivisia tunnisteita voidaan seurata Wi-Fi-reitittimillä. (CISCO Systems 2008.)

NFC-tunnisteet hyödyntävät samoja perustoiminan periaatteita kuin passiiviset RFID-tunnisteet. NFC-tunnisteiden eriytyminen perustuu NFC-tekniikan käyttöönottoon erilaisissa mobiililaitteissa. NFC-tekniikka ei varsinaisesti tarjoa parempaa tiedonsuojausta kuin RFID, mutta se hyödyntää erilaista dataformaattia. NFC-

tunnisteita voidaan käyttää samalla lailla kuin normaaleja passiivisia RFID-tunnisteita, vaikka useita erilaisia käyttösovelluksia on jo kehittynyt. Sovelluksista yksi näkyvimmistä ovat NFC-tekniikkaa hyödyntävät lähimaksukortit. (Chandler 2012.)

RFID- ja NFC-tunnisteiden koteloinnin pääsääntöinen tehtävä on suojella tunnisteen elektronisia komponentteja pölyltä, kosteudelta ja muilta ympäristön tuottamilta haitallisilta vaikutteilta. Tunnisteiden kotelointiin on olemassa runsaasti erilaisia vaihtoehtoja useilta eri valmistajilta. Koteloinnin muoto ja koko seuraa tunnisteen suurimman komponentin, joka on normaalisti antenni, vaatimuksia. Koteloinnin rakenteeseen vaikuttaa lisäksi tarkoitettu käyttökohde, esimerkiksi kulunvalvonnassa käytetyissä tunnisteissa on kotelointi suunniteltu avaimenperään kiinnitettäväksi. RFID-tunnisteiden kotelointitavoissa yleisimmin hyödynnetty materiaali on ABS-muovi, mutta koteloinnissa voidaan kuitenkin hyödyntää useita eri materiaaleja. (Finkenzeller, 2003, 13-21.) Kuviosta 7 voidaan nähdä erilaisia tunnisteiden kotelointitapoja.

Kuvio 7. Erilaisia RFID-tunnisteita ja niiden kotelointitapoja (Arnall 2007)



Kuvio 8. Röntgenkuvat neljästä eri NFC-lähimaksukortista (Minto 2014)

2.2.1 Mikroprosessori

RFID- ja NFC-tunnisteissa käytettyjen mikroprosessorien tehtävänä on pääsääntöisesti tiedonkäsittely ja radioaalloista, eli sähkömagneettisesta säteilystä, saadun vaihtovirran muuttaminen tasavirraksi. Kaikki mikroprosessorin tarvitsema tieto ja käyttövirta saadaan passiivisilla tunnisteilla antennin kautta, puolipassiivisilla ja aktiivisilla tunnisteilla taas sisäisen virtalähteen kautta. (Finkenzeller, 2003, 133-141.)

Kuviossa 9 esitellään tunnisteen mikroprosessorin vastaanottaman radioaallon käsittely sen sisäisissä toiminnoissa.

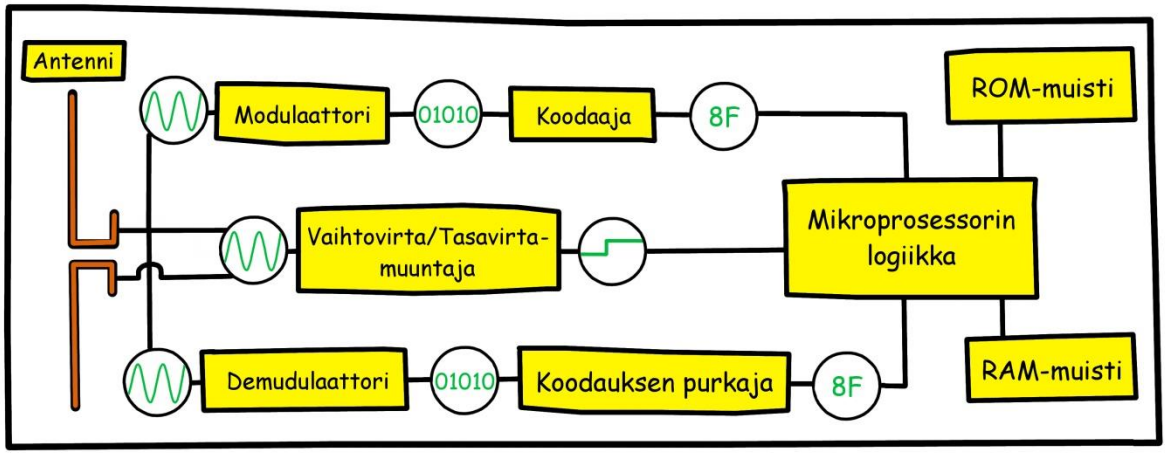
1. Vaihtovirta/Tasavirtamuuntaja tuo tarvittavan käyttövirran mikroprosessorille, joka aloittaa vastaanotetun radioaallon käsittelyn.

2. Vastaanotetun radioaallon modulaatio puretaan ja muutetaan saatu aaltokuvio binääridataksi.

3. Binääridatan koodaus puretaan mikroprosessorin logiikkapiirin ymmärtämään muotoon, joka voi olla esimerkiksi heksadesimaali muodossa.

4. Mikroprosessorin logiikka käsittelee saadun datan ja lähettää sen perusteella eteenpäin uutta dataa.

5. Datan lähetyksessä data ensin koodataan binääridataksi ja saadun binääridatan mukaan suoritetaan heijastettavan radioaallon modulointi. (TutorialsWeb [Viitattu 26.3.2015].)



Kuvio 9. Mikroprosessorin toiminnallinen lohkokaavio

2.2.2 Muisti

Tunnisteiden mikroprosessorien looginen toiminnallisuus ja digitaalinen tiedonkäsittely perustuvat olemassa oleviin toimintaohjeisiin, ohjelmointiin. Mikroprosessorin toimintaohjeet säilötään prosessorin valmistusvaiheessa pitkäkestoiseen muistiin, johon tallennettu ohjelmointi säilyy, vaikka tunnisteen sisäinen jännite laskisi nollaan. Mikroprosessorin ohjelmointiin käytetystä pitkäkestoisesta muistista käytetään yleisnimitystä ROM. ROM-muistin kehittyneemmät versiot ovat EPROM ja EEPROM, joissa muistien sisältö on uudelleenkirjoitettavaa. Moderneissa mikroprosessoreissa hyödynnetään EEPROM-muistia, joka voidaan tyhjentää elektroni-

sesti kun taas EPROM-muistin tyhjentämiseen tarvitaan voimakas ultraviolettivalo. (Corum 2005.)

ROM- ja EEPROM-muistit ovat verrattain hitaita ja kuluttavat toimintaansa nähden paljon virtaa, mikä tuottaa toiminnallisia ongelmia, jos niitä käytetään RFID tai NFC-tunnisteissa. Normaalisti ROM-muisti käsitetään nopeana muistina, mutta RFID-tunnisteiden edullisesta valmistuksesta johtuen niiden toiminnallisuus muuttuu merkitsevästi. Mikroprosessoreissa hyödynnetään tällöin lyhytkestoista muistia, joiden sisältö katoaa jännitteen laskiessa nollaan. Tällaista lyhytkestoista muistia kutsutaan RAM-muistiksi ja tunnisteissa sitä hyödynnetään laskennallisissa operaatioissa, joita voivat olla esimerkiksi tunnisteen salaukseen liittyvät toiminnot. Kuten ROM- myös RAM-muistista on olemassa erilaisia variaatioita, ja niiden hyödyntäminen mikroprosessoreissa otetaan nopeasti käyttöön. (Corum 2005.)

RFID- ja NFC-tunnisteet voidaan jakaa muistityyppien kirjoitettavuuden mukaan eri ryhmiin, mutta normaalisti luokkajaoissa otetaan huomioon useampi kuin yksi muuttuja. RFID-tunnisteet voidaan jakaa Auto-ID-standardien mukaan kuuteen ryhmään. Kyseistä standardointia käytetään yhä RFID-tunnisteiden luokkajaon pohjana. Tunnisteet jaetaan eri ryhmiin muistin ja virtaominaisuuksien erojen mukaan. (Poole [Viitattu 24.3.2015].) Taulukosta 3 voidaan nähdä Auto-ID-standardien mukainen luokkajako RFID-tunnisteille.

Taulukko 3. RFID-tunnisteiden luokkajako (Poole [Viitattu 24.3.2015])

Luokka	**Ominaisuudet**
Luokka 0	Passiivinen tunniste, jossa muistiin on kerran valmistuksen yhteydessä kirjoitettu. Voidaan vain lukea.
Luokka 1	Passiivinen tunniste, jossa muistiin voidaan kerran kirjoittaa. Voidaan vain lukea

Luokka 2	Passiivinen tunniste. Voidaan lukea ja kirjoittaa.
Luokka 3	Puolipassiivinen tunniste. Voidaan lukea ja kirjoittaa.
Luokka 4	Aktiivinen tunniste, joka sisältää erityisominaisuuksia.
Luokka 5	Aktiivinen tunniste, joka sisältää erikoisominaisuuksia, ja voi keskustella toisten saman luokan tunnisteiden kanssa.

NFC-tunnisteet voidaan puolestaan jakaa neljään eri ryhmään, joissa muuttujana toimii varsinainen muistikapasiteetti, muistityyppien kirjoitettavuus, tiedonsiirtonopeus tai ISO-standardi. (Poole [Viitattu 24.3.2015].) Taulukosta 4 voidaan nähdä luokkajako NFC-tunnisteille.

Taulukko 4. NFC-tunnisteiden luokkajako (Poole [Viitattu 24.3.2015])

Luokka	**Ominaisuudet**
Luokka 1	Perustuu ISO 14443A -standardiin. Voidaan kirjoittaa ja lukea, käyttäjä voi muuttaa vain luettavaksi. Perus muistikapasiteetti on 96 tavua, joka voidaan laajentaa 2 kilotavuun. Tiedonsiirtonopeus on 106 kilotavua sekunnissa.
Luokka 2	Perustuu ISO 14443A -standardiin. Voidaan kirjoittaa ja lukea, käyttäjä voi muuttaa vain luettavaksi. Perus muistikapasiteetti on 48 tavua, joka voidaan

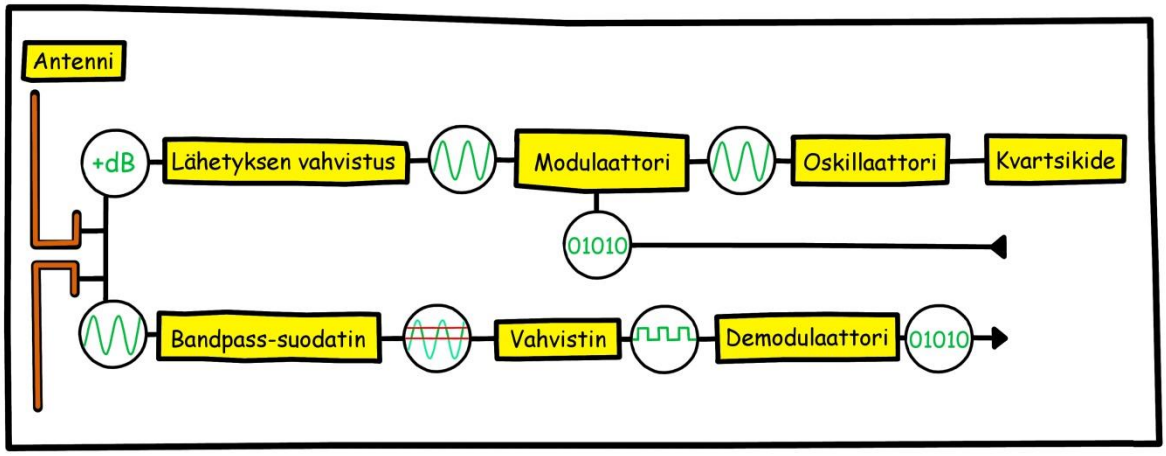
	laajentaa 2 kilotavuun. Tiedonsiirtonopeus on 106 kilotavua sekunnissa.
Luokka 3	Perustuu Sony FeliCa -järjestelmään. Voidaan vain lukea, kirjoitus tapahtuu valmistajan tai erikoislaitteiston toimesta. Perus muistikapasiteetti on 2 kilotavua. Tiedonsiirtonopeus on 212 kilobittiä sekunnissa. Sisältää erikoisominaisuuksia.
Luokka 4	Suunniteltu yhteensopivaksi ISO 14443A- ja B-standardien kanssa. Voidaan valmistajan esiasettaa valmistajan kertaalleen kirjoitettavaksi, käyttäjän kertaalleen kirjoitettavaksi tai uudelleen kirjoitettavaksi. Perusmuistikapasiteetti on 32 kilotavua. Tiedonsiirtonopeus on 106–424 kilotavua sekunnissa.

2.3 Lukija

Lukija on RFID- tai NFC-järjestelmän ylläpitäjälle kuuluva osa. NFC-tekniikkaa hyödyntävissä mobiililaitteissa, kuten matkapuhelimissa ja tableteissa, katsotaan käyttäjän ja ylläpitäjän jakavan samoja ominaisuuksia. Lukijan yksinkertaistettu tehtävä on toimia erimuodoissa tunnisteen ja ylläpitävän järjestelmän välissä. Lukijan tärkein tehtävä on tuottaa tunnisteen toiminnalle tarvittava käyttövirta radioaaltojen kautta, ja tätä kautta aktivoida tunniste. Tunnisteen aktivoituessa ja lähettäessä sisältämänsä datan lukija vastaanottaa ja lähettää sen eteenpäin ylläpitävälle järjestelmälle, joka puolestaan prosessoi saadun datan ja suorittaa tarpeelliset jatkotoiminnot. Lukija voi tarpeen tullen myös kirjoittaa tunnisteelle dataa ylläpitävän järjestelmän ohjeiden mukaan. (Finkenzeller, 2003, 309.)

Lukija koostuu kahdesta osasta, jotka ovat transponderi eli lähetin-vastaanotin ja hallintalaitteisto. Transponderin tehtävänä on pääsääntöisesti vastaanottaa aktivoidun tunnisteen lähettämää dataa ja välittää käsitelty binäärimuotoinen data hal-

lintalaitteistolle. Lähetystoiminnassa transponderi moduloi hallintalaitteistolta saadun binäärimuotoisen datan ja lähettää sen eteenpäin. (Finkenzeller, 2003, 309-316.) Kuviosta 10 voidaan nähdä esimerkki kuinka transponderi käsittelee vastaanottamansa datan.



Kuvio 10. Transponderin datan käsittely

Hallintalaitteiston toiminnat keskittyvät transponderilta saadun datan käsittelyyn ja sen välittämiseen hallintajärjestelmälle. Yksinkertaisimmillaan hallintalaitteisto vastaanottaa binäärimuotoisen datan ja purkaa sen järjestelmän ymmärtämään muotoon ja lähettää eteenpäin. Kuitenkin moderneissa järjestelmissä hallintalaitteiston tehtäviin voi kuulua useiden tunnisteiden yhtäaikaisen käsittelyn hallinta, salauksen purku ja luominen sekä tunnisteen ja lukijan välinen varmennus, jonka avulla voidaan estää järjestelmään kuulumattomien tunnisteiden käsittely hallintajärjestelmässä. (Finkenzeller, 2003, 316-317.)

Kuviossa 11 esitellään esimerkki RFID-lukijan toiminnasta:

1. Transponderin antenni tai kela vastaanottaa tunnisteen kantoaallosta moduloidun signaalin.

2. Vastuksista ja kondensaattoreista muodostuva Bandpass-suodatin poistaa vastaanotetusta signaalista liian korkeat ja matalat taajuudet.

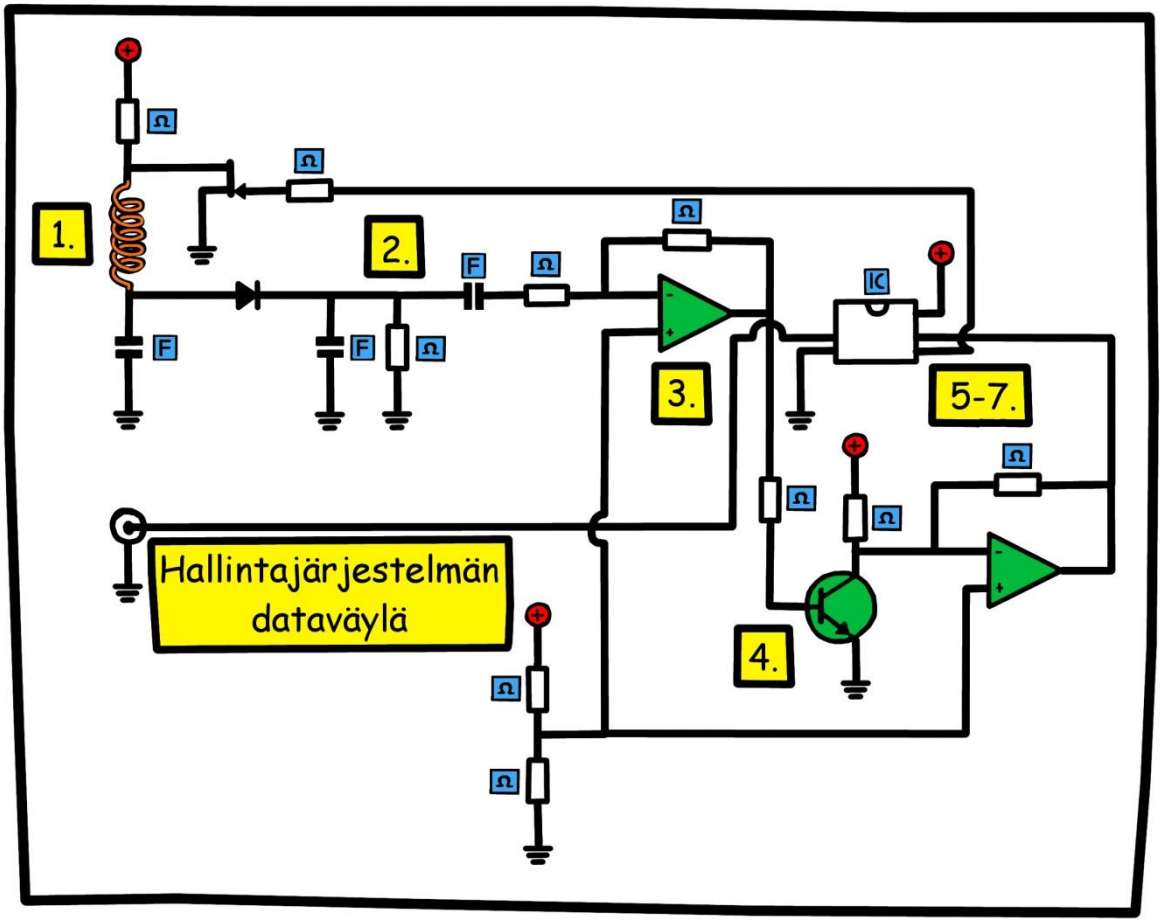
3. Negatiivisella takaisinkytkennällä vahvistetaan signaalin voimakkuutta vahvistimessa.

4. Signaalin saavuttaessa huippukohtansa transistori aktivoituu ja päästää virtaa läpi.

5. Transistorin aktivoituessa virta kulkee myös vahvistimen läpi, joka vahvistaa ja asettaa yksittäisen mikroprosessorin pinnin HIGH-tilaan, muutoin pinnin on LOW-tilassa.

6. Mikroprosessori käsittää HIGH-tilan binäärimuotoisena merkkinä 1 ja LOW-tilan merkkinä 0.

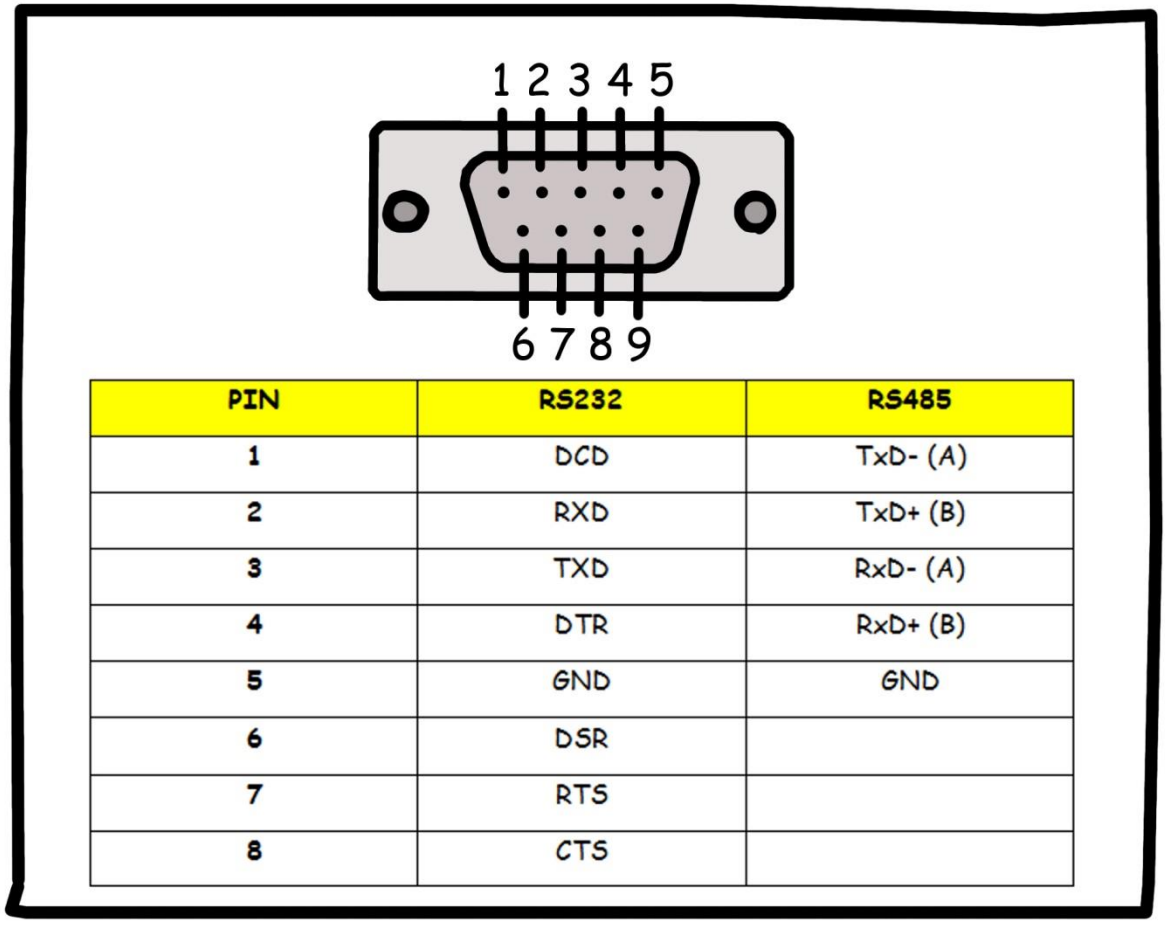
7. Mikroprosessori vastaanottaa tunnisteen lähetetyn signaalin sarjana binäärimuotoisia merkkejä.



Kuvio 11. RFID-lukijan toiminta

Lukijan yksi tärkeimmistä ominaisuuksista on toimia tiedonsiirtoväylä lukijan ja hallintajärjestelmän välillä. Tiedonsiirtoväylää hyödynnetään useissa lukijan toiminnoissa, esimerkiksi tunnisteen varmentamisessa tai järjestelmän salausavaimen

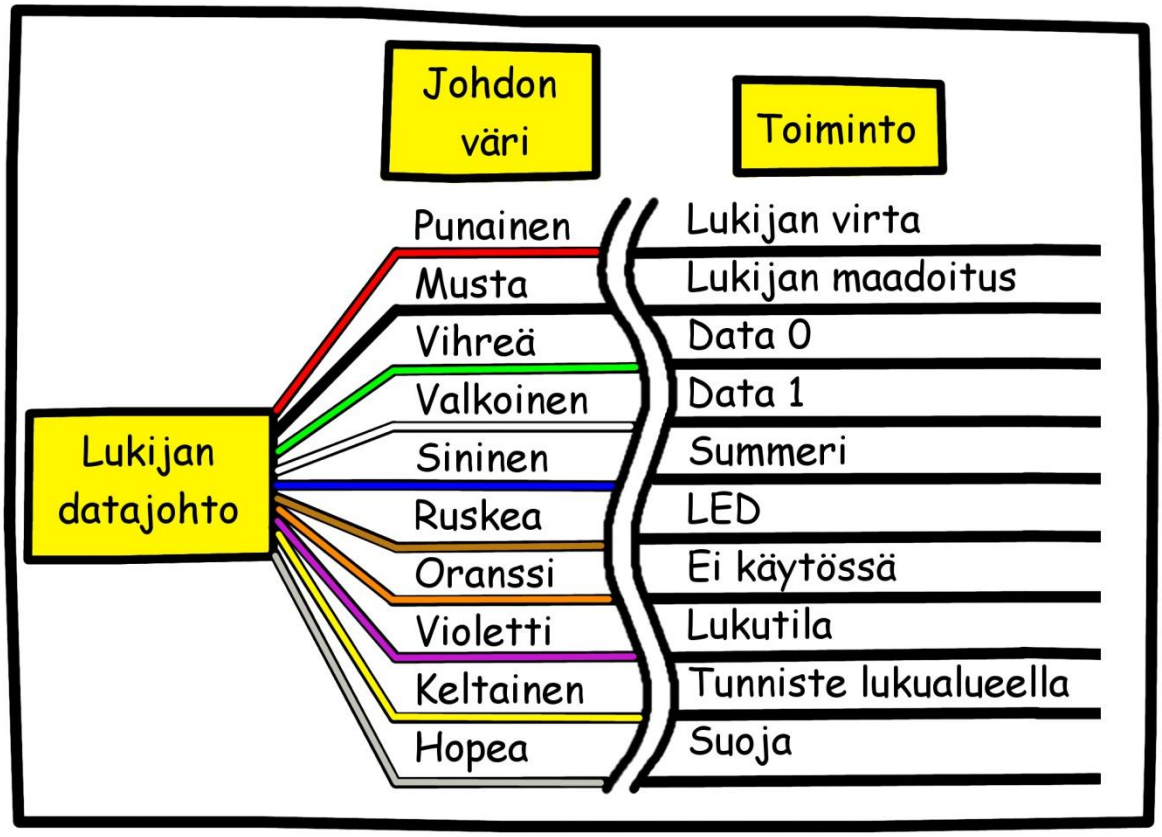
jakamisessa, lukijan toiminnan varmistamisessa. Tiedonsiirtoväylänä voidaan käyttää esimerkiksi RS232. tai RS485-väylää. (Finkenzeller, 2003, 316-317.) Kuviossa 12 esitellään RS232- ja RS485-väylien johdotus.



PIN	RS232	RS485
1	DCD	TxD- (A)
2	RXD	TxD+ (B)
3	TXD	RxD- (A)
4	DTR	RxD+ (B)
5	GND	GND
6	DSR	
7	RTS	
8	CTS	

Kuvio 12. RS232- ja RS485-tiedonsiirtoväylien johdotus

Yleisimmin käytetty tiedonsiirtoväylä on Wiegand, jota hyödynnetään lähes kaikissa RFID-lukijoissa. Wiegand-protokollalla voidaan käsittää useita eri asioita, mutta tässä yhteydessä sillä tarkoitetaan lukijan ja hallintajärjestelmän välistä fyysistä tiedonsiirtotapaa. Wiegandin käyttäminen ei rajoitu ainoastaan RFID- tai NFC-kulunvalvontalukijoihin, vaan sitä hyödynnetään lähes kaikissa kulunvalvonnan lukijoissa, kuten esimerkiksi sormenjälkitunnistimissa. (Franken 2008.) Kuviossa 13 voidaan nähdä esimerkki Wiegand-väylän johdottamisesta. Johdotuksessa voidaan käyttää tapauskohtaisesti vain osaa johdoista.



Kuvio 13. Wiegand-tiedonsiirtoväylän johdotus

Matkapuhelimissa ja muissa mobiililaitteissa yleistynyt NFC mahdollistaa laitteiden hyödyntämisen NFC-lukijana, laitteiden salliessa niin tunnisteen lukemisen ja kirjoittamisen. NFC-tekniikkaa voidaan verrata Bluetooth-tekniikkaan, ottaen huomioon, että bluetooth tarjoaa lähes 50 metrin käyttöetäisyyden kun taas NFC alle 10 senttimetrin etäisyyden. NFC-tekniikkaa hyödynnetään lyhyen lukuetäisyyden takia erilaisissa tietoturvaa vaativissa yhteyksissä ja sovelluksissa. (Poole [Viitattu 24.3.2015].)

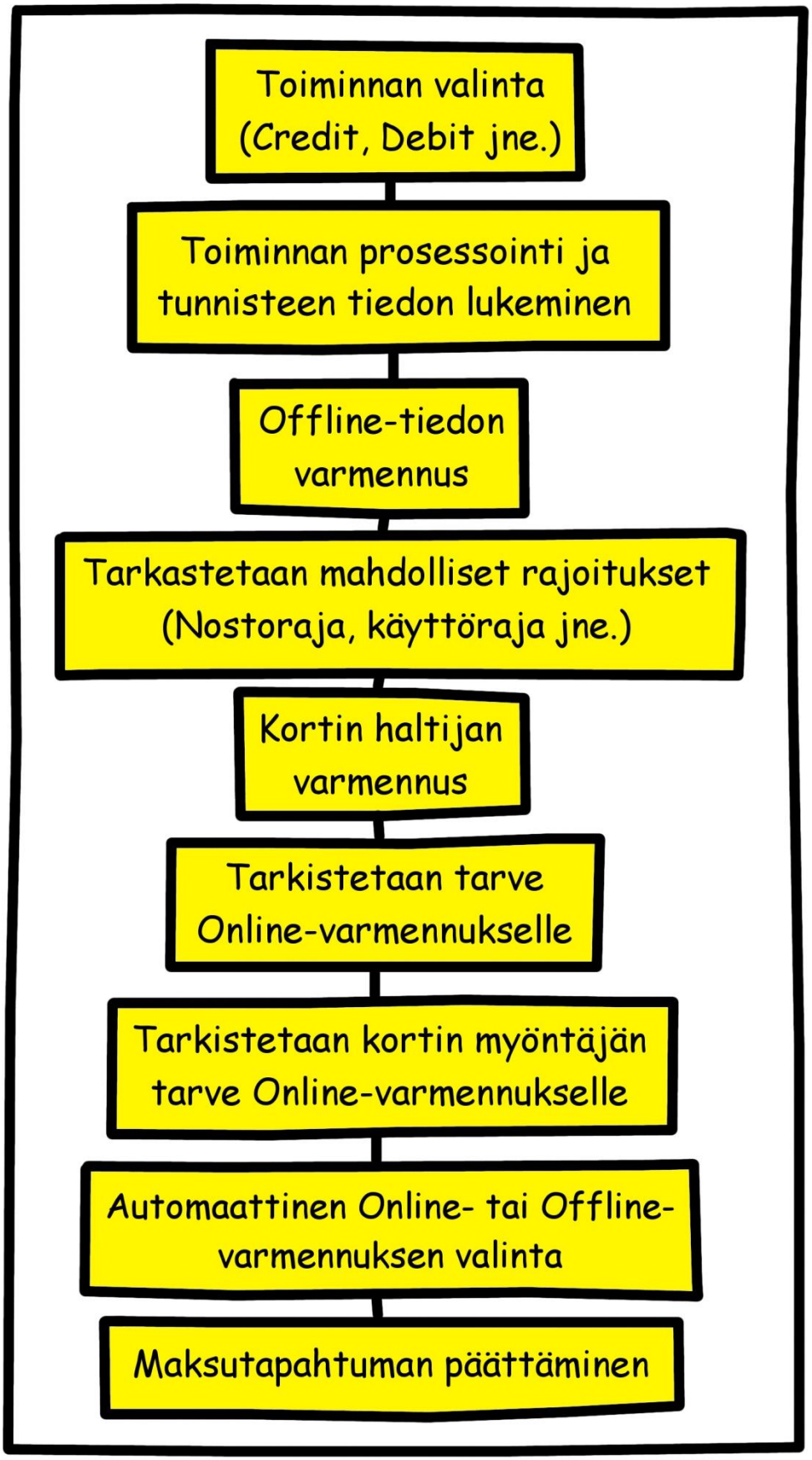
2.4 Hallintajärjestelmä

Hallintajärjestelmä on RFID-järjestelmän ylläpitäjälle kuuluva osa. Hallintajärjestelmän pääsääntöiset tehtävät perustuvat tietorekisterin ylläpitämiseen, johon on tallennettu tunnisteita vastaavat tiedot. Hallintajärjestelmä on normaalisti yksittäinen keskustietokone, jonka kautta ylläpitäjä voi tarvittaessa syöttää uusia tunnisteita rekisteriin, poistaa vanhoja tai tarkastella tunnistehistoriaa. Hallintajärjestel-

mää käytetään tietokonepäätteeltä hyödyntämällä erikseen tarkoitukseen suunniteltua käyttöliittymää.

Hallintajärjestelmä voidaan jakaa kahteen eri pääryhmään toiminnallisuutensa mukaan: online- ja offline-järjestelmään. Online-järjestelmä on perinteinen keskustietokoneeseen nojautuva hallintajärjestelmä, jossa tieto kulkee lukijoilta keskustietokoneelle. Offline-järjestelmä taas ei hyödynnä keskustietokonetta toiminnassaan, vaan lukijalla itsessään on lista sallituista tunnisteista. Tunnisteiden hallinta vaihtelee näillä kahdella eri tyypillä huomattavasti. Online-järjestelmässä tunnisteiden oikeuksia voidaan muuttaa keskustietokoneelta käsin, kun taas offline-järjestelmässä tunniste pitää fyysisesti kirjoittaa uudelleen tai mahdollisesti jopa tuhota. (Finkenzeller, 2003, 357-359.)

NFC-tekniikkaa hyödynnetään lähimaksukorteissa, joiden maksutapahtumaan perustuva hallintajärjestelmä on monitahoinen. Lähimaksukorttien maksutapahtuma ei eroa huomattavalla tavalla sirukortillisten maksukorttien maksutapahtumasta, jossa maksutapahtuma voidaan jakaa yhdeksään eri osaan aina kortin havaitsemisesta maksutapahtuman päättämiseen. (EMVCo 2011.) Kuviossa 14 esitellään maksukorttien maksutapahtuma, jossa online-järjestelmällä viitataan internetin kautta yhteydessä olevaan pankkijärjestelmään ja offline-järjestelmällä maksuterminaalin paikalliseen toimintaan.



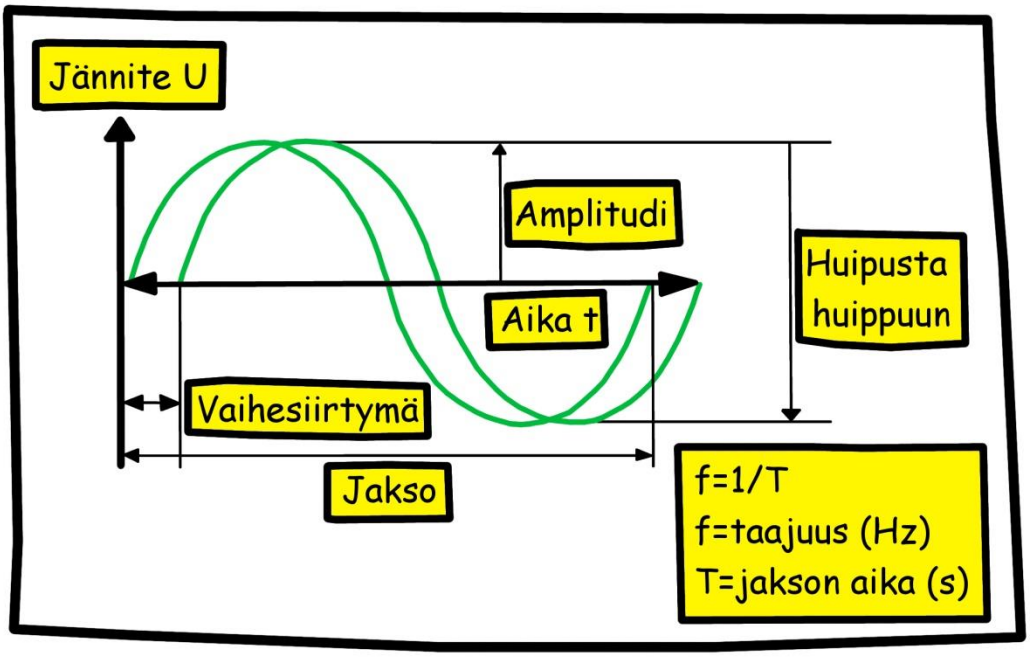
Kuvio 14. Maksukorttien maksutapahtuma

2.5 Tiedonsiirto

Tässä osiossa käsitellään yleisellä tasolla RFID- ja NFC-tekniikassa hyödynnettävät tiedonsiirtotavat. Lisäksi käsitellään tunnisteen ja lukijan välinen tiedonsiirto ja siirrettävän datan rakenne, sekä lukijan ja hallintajärjestelmän välinen tiedonsiirto ja datarakenne.

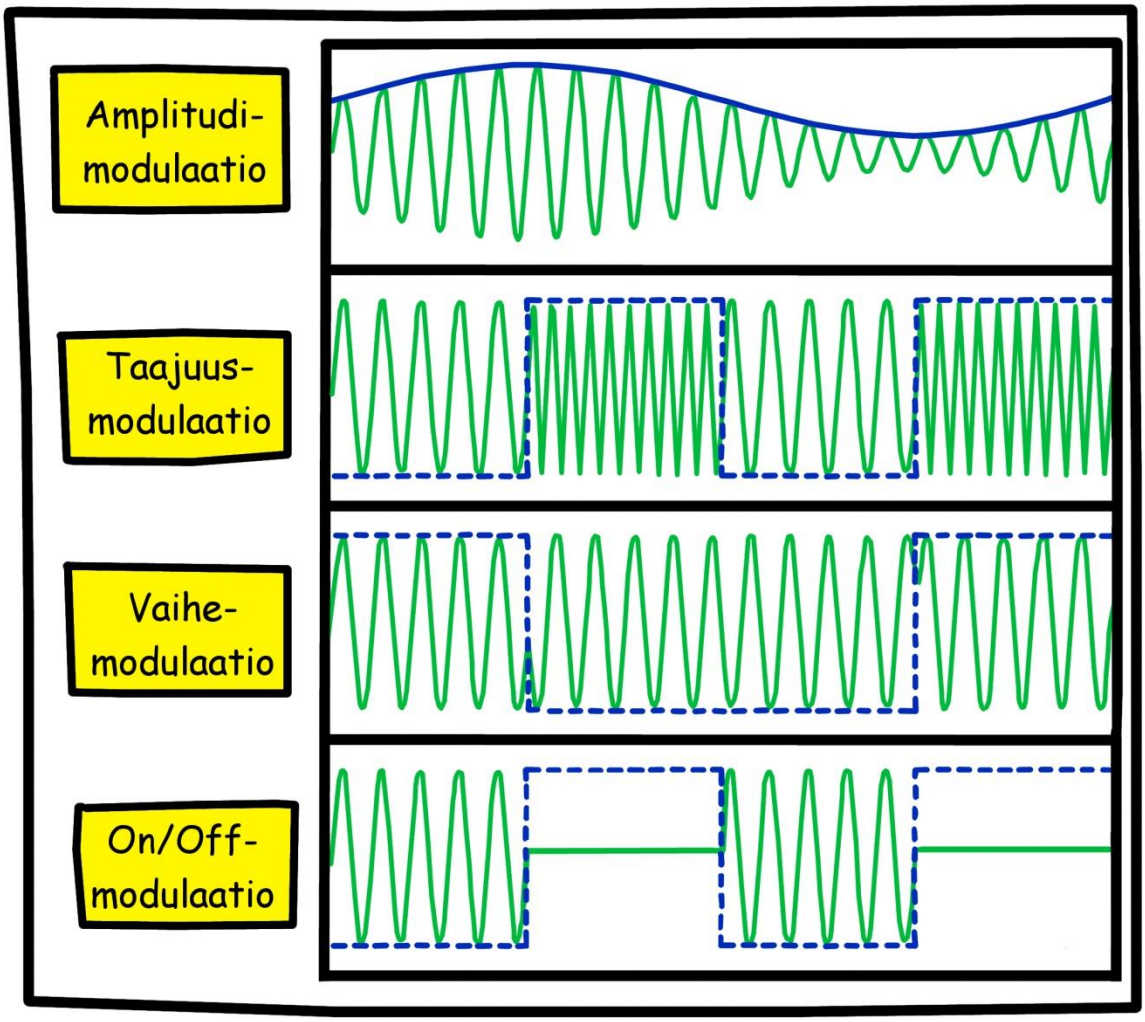
2.5.1 Modulaatio

Tietoliikenne lukijan ja tunnisteen välillä tapahtuu sähkömagneettista kantoaaltoa moduloimalla, aktiivisissa tunnisteissa tunniste tuottaa oman kantoaaltonsa. Moduloinnilla tarkoitetaan yksittäisen signaalin muokkaamista toisella signaalilla, jolloin saadaan aikaan kahden signaalin yhdistelmä. RFID- ja NFC-tekniikan passiivisiin tunnisteisiin perustuvissa järjestelmissä modulaation pohjana toimivan analogisen kantoaallon lähettää lukija, johon tunniste tekee omat muutoksensa moduloimalla siihen ennalta määritellyssä formaatissa digitaalista dataa. Digitaalisen signaalin modulointi analogiseen kantoaaltoon suoritetaan vaikuttamalla yhteen sähkömagneettisen aaltoliikkeen kolmesta ominaisuudesta eli amplitudiin, taajuuteen tai jaksoon. (Finkenzeller, 2003, 183.) Kuviosta 15 voidaan nähdä esimerkit.



Kuvio 15. Amplitudin, taajuuden ja jakson esimerkit

Yleisimmät RFID-tekniikoissa käytettävät modulaatiot pohjautuvat modulaatioihin ASK (Amplitude-Shift Keying), FSK (Frequency-Shift Keying), PSK (Phase-Shift Keying) ja harvinaisissa tapauksissa OOK (On/Off Keying). ASK-tavassa eli amplitudimodulaatiossa muutoksen kohteena on kantoaallon amplitudi eli aallonkorkeus. FSK-tavassa eli taajuusmodulaatiossa muutoksen kohteena on kantoaallon taajuus. PSK-tavassa eli vaihemodulaatiossa muutoksen kohteena on kantoaallon vaihe. OOK-tavassa eli päälle/poismodulaatiossa muutoksen kohteena on signaalin varsinainen lähettäminen. Usein käytetään vain yhtä modulointitapaa, mutta erikoistapauksissa voidaan hyödyntää useampia modulointitapoja. (Thompson, 2008.) Kuviossa 16 esitellään esimerkit käytetyistä modulaatiotavoista.



Kuvio 16. Modulaatioesimerkkejä

Lukijalta tunnisteelle lähetettävä kantoaalto voidaan tarvittaessa moduloida, mutta tällöin täytyy ottaa huomioon passiivisten tunnisteiden ominaisuus ottaa toiminta-virtansa vastaanotettavasta kantoaallosta (Thompson, 2008).

NFC-tekniikassa hyödynnetään pääasiassa ASK-modulaatiota. Passiivisissa NFC-laitteissa hyödynnetään 10 % modulaatiota, kun taas aktiivisissa 100 % modulaatiota. (Poole [Viitattu 24.3.2015].)

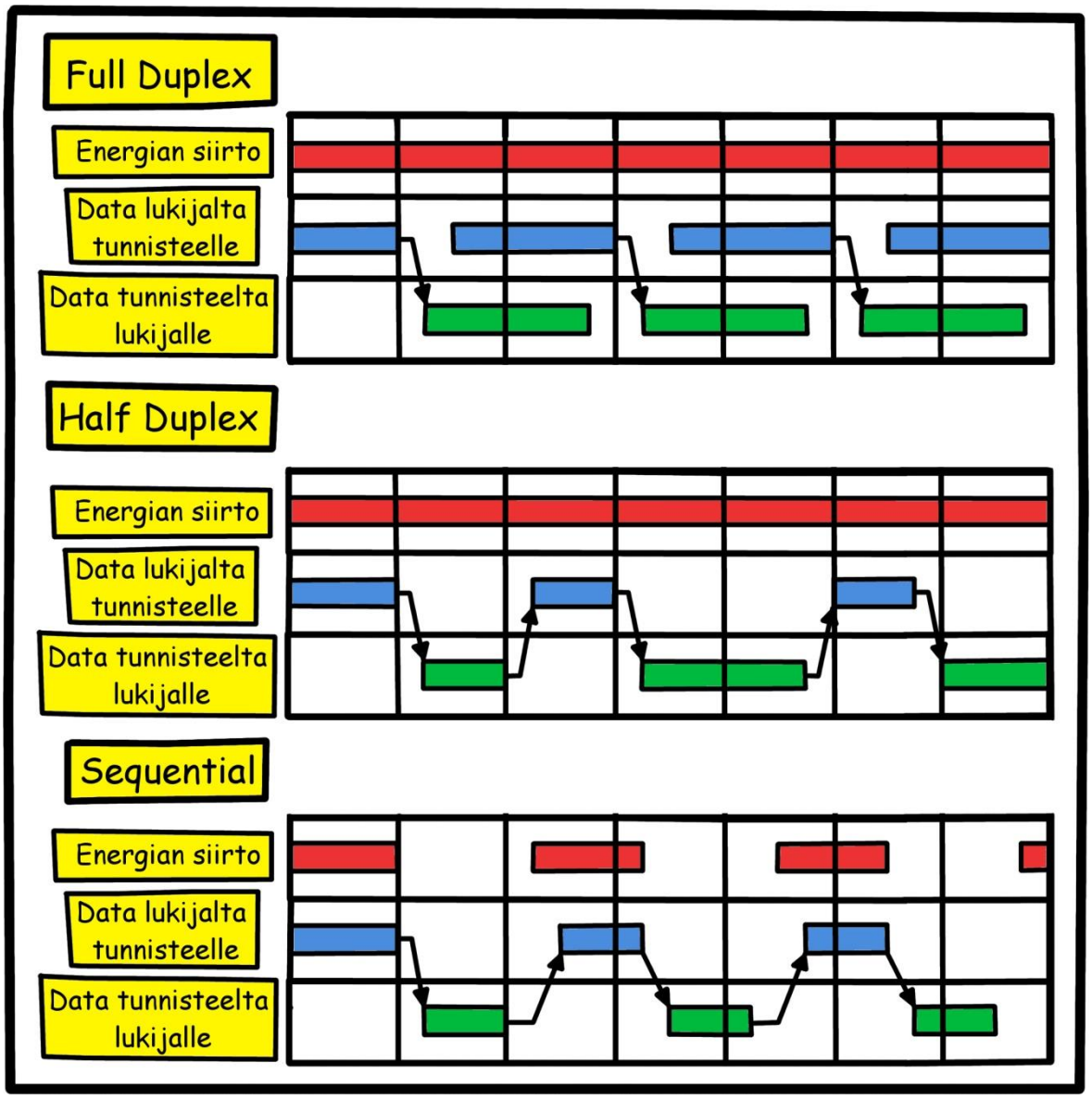
2.5.2 Tietoliikenteen vuorottelu

Tietoliikenteen suuntauksella tarkoitetaan lukijan ja tunnisteen välisen tietoliikenteen lähetysvuorottelua. RFID-tekniikassa käytettävät lähetysvuorottelut ovat Full Duplex, Half Duplex ja Sequential. (Finkenzeller 2003, 40-41.)

Full Duplex -vuorottelussa lukija tarjoaa jatkuvasti tunnisteen toiminnalleen tarvitseman energian. Lukijan ja tunnisteen välinen tiedonsiirto tapahtuu yhtäaikaisesti, jolloin tunniste lähettää dataa eri taajuudella. Tunnisteen käyttämä taajuus on normaalisti tietyn muuttujan verran pienempi kuin lukijan lähettämä, koska tunniste ei pysty kasvattamaan vastaanottamaansa taajuutta. (Finkenzeller 2003, 40-41.)

Half Duplex -vuorottelussa lukija tarjoaa jatkuvasti tunnisteen toiminnalleen tarvitseman energian. Lukijan ja tunnisteen välinen tiedonsiirto tapahtuu vuorotellen käyttäen samaa taajuutta. (Finkenzeller 2003, 40-41.)

Sequential-vuorottelussa lukija lähettää datan ja tunnisteen toiminnalleen tarvitseman energian samanaikaisesti. Tunniste lähettää dataa kun lukija ei lähetä dataa tai energiaa. Tätä vuorottelutapaa hyödyntävät tunnisteet käyttävät kondensaattoreita hetkellisinä energiapankkeina saaden näin taukotilojen ajaksi toiminta-virtaa. (Finkenzeller, 2003, 40-41.) Kuviosta 17 voidaan nähdä esimerkit erilaisista tietoliikenteen vuorottelutavoista.



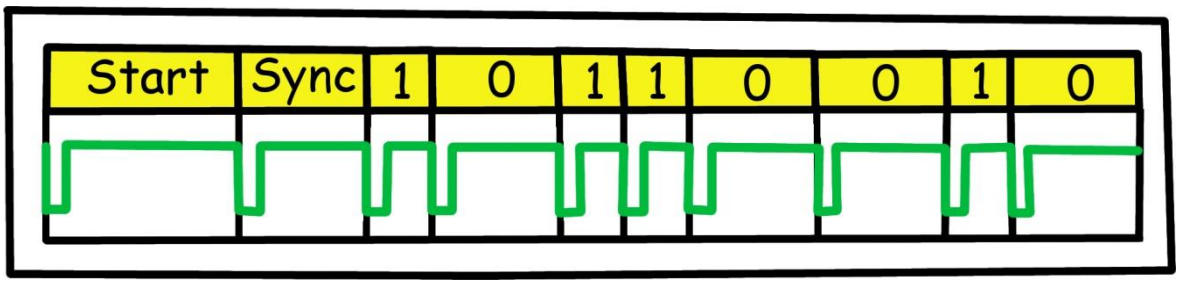
Kuvio 17. Esimerkit erilaisista vuorottelutavoista

2.5.3 Signaalin digitaalinen koodaus

Kantoaaltoon moduloitu digitaalinen signaali pyritään suunnittelemaan liikkumis-suuntakohtaisesti. Tämä tarkoittaa sitä, että lukijalta tunnisteelle ja tunnisteelta lukijalle välitettävän kantoaallon modulaatio ja digitaalinen koodaus suoritetaan ottaen huomioon niin lähettäjän että vastaanottajan ominaisuudet. (Thompson 2008.)

Lukijan tehtäviin kuuluu joissain tapauksissa lähettää tunnisteelle koodisarja, josta tunniste tietää aloittaa oman lähetyksensä. Tunnisteelle lähetettävä kantoaalto

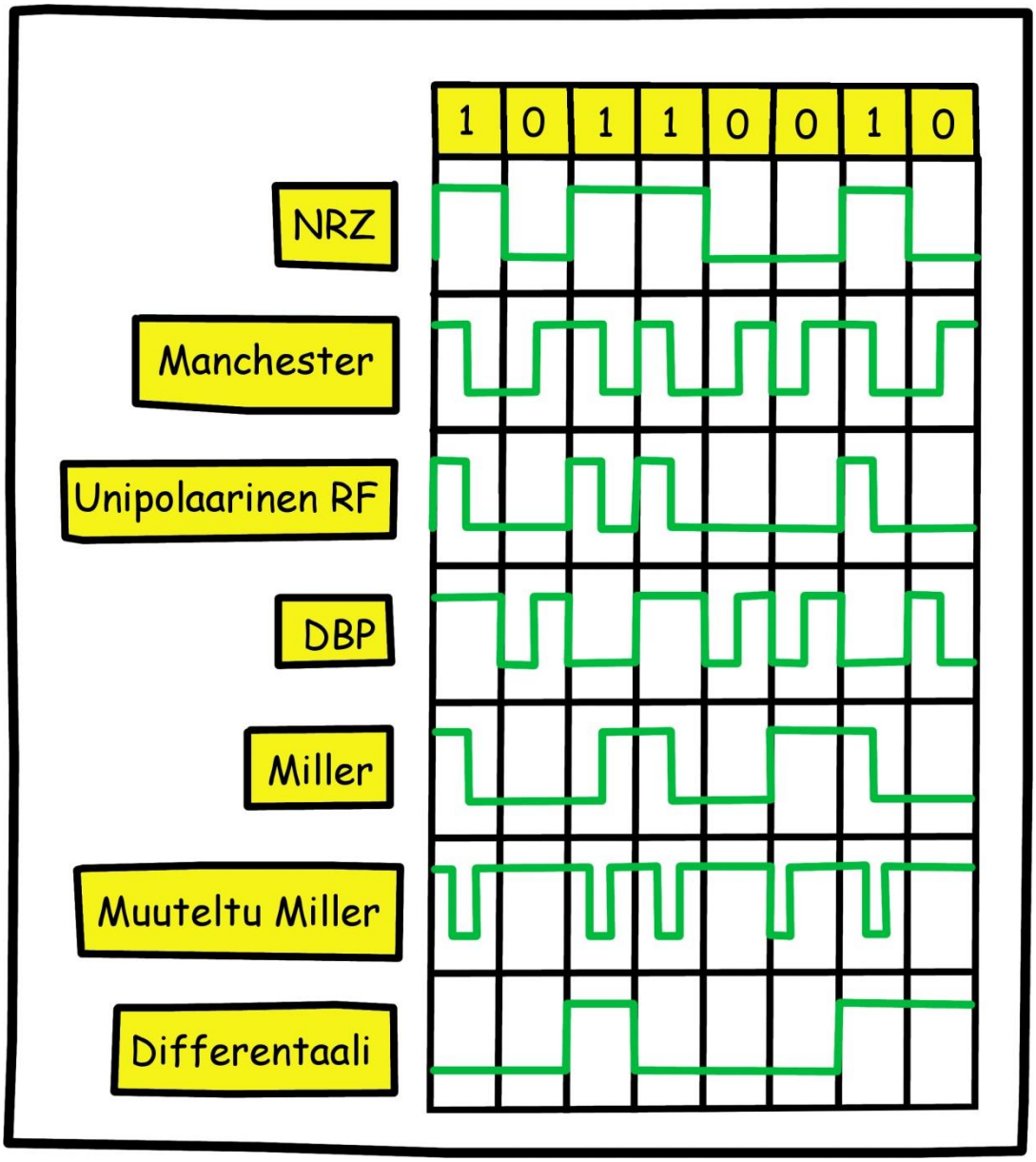
pyritään pitämään lähtökohtaisesti mahdollisimman yhtenäisenä, näin pidetään tunnisteen kantoaallosta ottama toimintavirta mahdollisimman suurena. Lukijan lähettämä kantoaalto pyritään pitämään siis mahdollisimman muuttumattomana. Lähetetyn moduloidun kantoaallon digitaalisessa koodauksessa voidaan hyödyntää esimerkiksi PPC-koodausta, se mahdollistaa mahdollisimman suuren toimintavirran tunnisteelle. (Thompson 2008.) Kuviosta 18 voidaan nähdä PPC-koodauksen esimerkki.



Kuvio 18. PPC-koodauksen esimerkki

Tunnisteen lähettämän moduloidun kantoaallon digitaalisessa koodauksessa pyritään myös toimimaan mahdollisimman energiatehokkaasti ja sallia näin mikroprosessorin suurempi virrankulutus. Puolipassiivisissa ja aktiivisissa tunnisteissa ei virrankulutuksellisesti olisi tarvetta toimia energiatehokkaasti, mutta samoja koodaustapoja hyödyntäen voidaan kuitenkin pidentää sisäisen virtalähteen elinikää. Tunnisteen moduloinnissa ei tarvitse myöskään ottaa huomioon moduloidun kantosignaalin virransiirtokykyä. (Finkenzeller 2003, 184-186.)

Kantoaaltoon moduloitavan digitaalisen signaalin koodaukseen on olemassa useita eri vaihtoehtoja, joista useasta on muodostettu muunneltuja versioita. Osa koodauksista toimii vain tietyillä modulaatiotavoilla. (Finkenzeller 2003, 184-186.) Kuviosta 19 voidaan nähdä yleisimmät koodaustavat. Näiden lisäksi voidaan hyödyntää myös edellä mainittua PPC-koodausta.



Kuvio 19. Yleisimpien koodaustapojen esimerkit

On kuitenkin huomioitava, että eri valmistajat hyödyntävät useasti eri koodaustapoja ja -tyyppejä. Standardisoinnilla on kuitenkin pyritty vaikuttamaan modulaation ja koodauksen monimuotoisuuteen. Esimerkiksi EPCglobalin Class-1 Generation-2 -protokollassa määritellään muun muassa modulaatiot ja koodaukset UHF RFID -järjestelmille, samaa standardia on myös hyödynnetty muissakin tunnisteissa ja järjestelmissä. (EPCglobal 2005.)

2.5.4 Datarakenteet

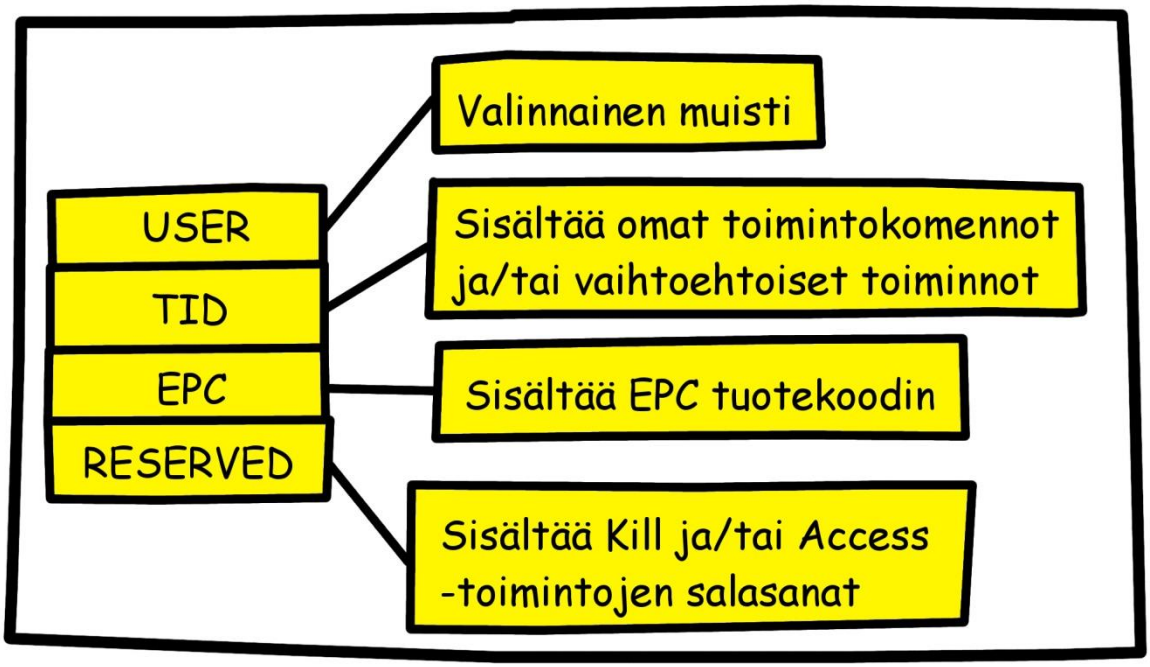
RFID- ja NFC-tunnisteella oleva tieto voidaan tallentaa usealla eri tavalla, mutta jokaiseen tapaan vaikuttaa oleellisesti tunnisteen tarjoama muistin määrä. Muistin määrän yksikkönä toimii bitti, jolla voi olla 1- tai 0-tila. Näiden arvojen avulla luodaan binäärilukusarjoja, jotka voidaan tarvittaessa kääntää takaisin ymmärrettävään desimaali- tai ASCII-muotoon. Tunnisteissa ilmoitetaan yleensä suurin sallittu datamäärä bitteinä, joiden määrän mukaan voidaan tarkastella kuinka monta eri tilaa voidaan biteistä muodostaa. (Sherz 2007.) Taulukossa 5 esitellään bittien ja tilamäärien vertaaminen.

Taulukko 5. Bittien ja tilamäärän vertaaminen

Bitti		Tilaa
1	2^1	2
2	2^2	4
4	2^4	16
8	2^6	256
16	2^16	65 536
32	2^32	4 294 967 296
64	2^64	18 446 744 073 709 551 601

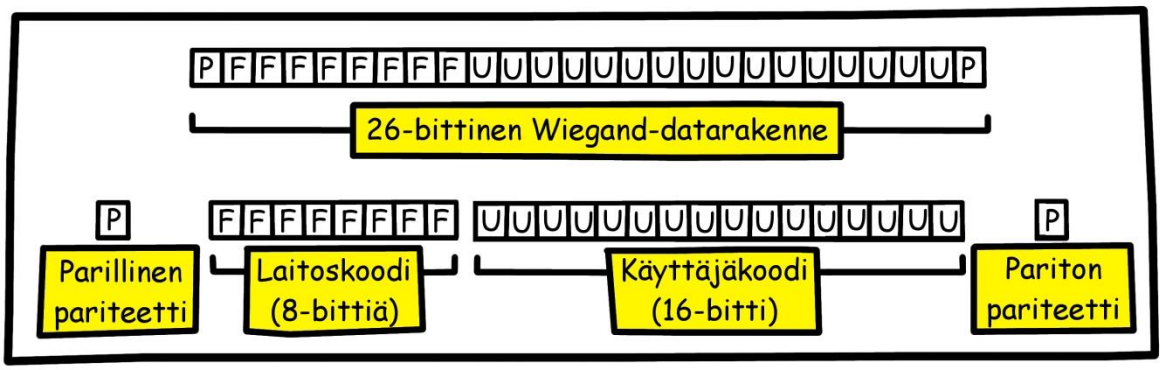
Tällä hetkellä markkinoilla olevien tunnisteiden muistikapasiteetti voi vaihdella 1 bitistä aina noin 66 kilobittiin. Esimerkiksi helmikuussa 2014 MAINtag-tunnistevalmistaja julkaisi FLYchip64-mikroprosessorin UHF-taajuuden tunnisteisiin. Kyseisen mikroprosessorin käyttäjälle varattu muistikapasiteetti on yli 65 kilobittiä. (MAINtag 2014.)

Tunnisteille tallennettu data jaetaan yleensä tietyn kokoisiin lohkoihin, joihin tallennetaan erityyppistä dataa. Näistä lohkoista muodostetaan varsinainen datarakenne. Yleisimmät RFID-tunnisteissa käytetettyjen datarakenteiden tyypit ovat EPC-globalin Class-1 Generation-2- ja Wiegand-rakenne. Class-1 Generation-2-, tai Gen 2 -tunnisteiden rakenne koostuu neljästä eri datapankista. Gen 2 -rakenne on suunniteltu erityisesti logistiikan tarpeisiin, mutta sitä voidaan hyödyntää myös datan siirrossa eikä sille ole määritelty suurinta mahdollista datamäärää. (EPCglobal 2013.) Kuviosta 20 voidaan nähdä Gen 2 -rakenteen esimerkki.



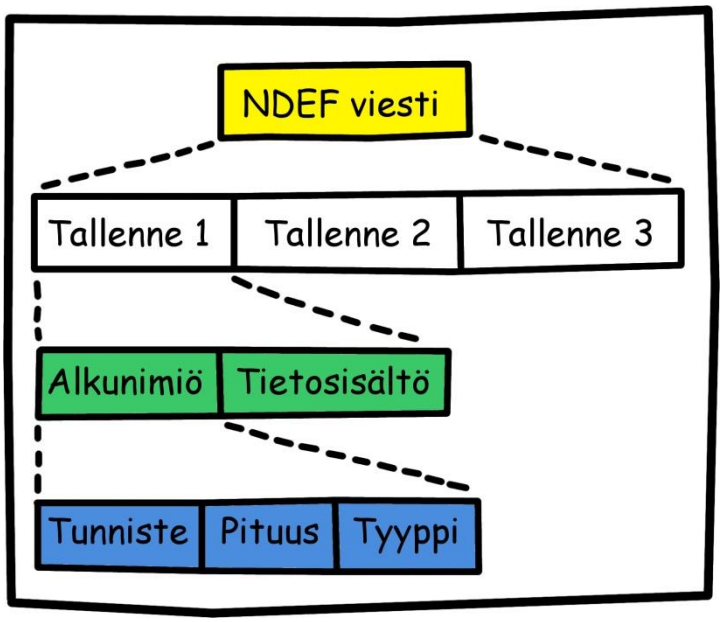
Kuvio 20. EPC Gen 2 -rakenne

Wiegand-rakenne on hyvin yleinen kulunvalvonnan sovelluksissa käytetty tiedon tallennustapa. Rakenne määrittelee kuinka dataa tallennetaan tunnisteen muistiin, mutta ei kuitenkaan määritellä varsinaista datan määrää. Wiegand-standardi taas tarkoittaa yleisessä käytössä olevaa 26-bitin tiedontallennusformaattia. Kyseinen 26-bitin tallennusformaatti on yleisesti saatavilla oleva ja helposti implementoitava, mistä johtuu että se on yksi eniten kulunvalvonnassa käytetyistä formaateista. (HID 2006.) Kuviosta 21 voidaan nähdä Wiegand-datarakenteen esimerkki.



Kuvio 21. 26-bittisen Wiegand-datarekenteen esimerkki.

NFC-tunnisteissa käytetään NCF Forumin kehittämää NDEF-rakennetta tai siitä kehitettyä SNEP-rakennetta. NDEF-rakenne koostuu yhdestä tai useammasta tallenteesta, joiden välinen erotus tehdään hyödyntämällä ensimmäisen tallenteen arvoja, joista voidaan päätellä koska ensimmäinen tallenne loppuu ja toinen alkaa. (NFC Forum 2006.) Kuviosta 22 voidaan nähdä NDEF-viestin rakenne.



Kuvio 22. NDEF-viestin rakenne

Lähimaksukorteissa hyödynnetään EMV:n omaa rakennetta, joka perustuu kysely-vastaus-toiminnalle, jossa lähimaksukortille on tallennettu dataa tiedostorakenteeseen. Kyseinen data on tallennettu tiedostorakenteeseen ennalta määrätyille paikoille, josta challenge-response-järjestelmää hyödyntäen haetaan tarvittavat tiedot. (EMVCo 2011.)

3 TIETOTURVA

Tässä osuudessa käsitellään mahdolliset tietoturvat joita voidaan hyödyntää RFID- ja NFC-tekniikassa, sekä esimerkkitapauksia jo julkisesti esitellyistä murto- ja hyödyntämistekniikoista. Tarkastelun kohteena on erityisesti kulunvalvonnassa käytetty RFID-tekniikka ja siihen pohjautuvat turvatekniset ratkaisut sekä NFC-tekniikkaan pohjautuva lähimaksutekniikka.

Esimerkeissä käytetyt murto- tai hyödyntämistekniikat on joko esitetty julkisissa tietoturvatapahtumissa tai niistä on julkaistu julkisia tutkimusraportteja.

3.1 Käytettävissä oleva tietoturva

Ymmärrettävää on että logistiikan tarpeisiin kehitetyssä RFID-järjestelmässä ei ole ollut tarvetta suojata tunnisteen lähettämää dataa. Tämä mahdollistaa tiedon helpomman luettavuuden, mutta tekniikan siirtyessä käsittämään turvatekniikan, kulunvalvonnan ja maksukorttien sovelluksia on tietoturvan tarve konkretisoitunut. (Suprina, 2005.)

RFID- järjestelmien mahdolliset tietoturvaratkaisut voidaan jakaa useisiin eri tapoihin ja tekniikoihin, joita yhdistelemällä voidaan luoda tietoturvallisesti luotettavia kokonaisuuksia. Tietoturvassa yleisesti tärkeimmät suojausmetodit pohjautuvat todennukseen, salaukseen, pseudonymisaatioon sekä lukemisen estämiseen. (IZT, Empa & BSI 2004.)

3.1.1 Todennus

Todennus ja salaus ovat hyvin samankaltaisia toimintamenetelmiä. Todennuksella pyritään varmistamaan käyttöoikeus ja sallittu tiedonsiirto, kun taas salauksella pyritään turvaamaan tietoliikenne lukulaitteen ja tunnisteen välillä. (IZT, Empa & BSI 2004.)

Todennuksella voidaan esimerkiksi varmistaa, onko tunnisteella oikeudet lukulaitteen yhteyteen lisättyyn toimintoon. Korkean tietoturvan vaativissa yhteyksissä on tärkeää varmistaa lukija tunnisteelle eikä ainoastaan tunniste lukijalle. On hyvä huomata, että korkean tietoturvan RFID-järjestelmissä tulisi myös aina todentaa lukija hallintajärjestelmälle. (IZT, Empa & BSI 2004.)

Kun RFID-järjestelmä kohtaa tunnisteen sen, täytyy varmistaa että kyseessä olevan tunnisteen lähettämä tunnistekoodi vastaa järjestelmän rekisterissä olevaa. Näin pyritään ehkäisemään väärennettyjen tai kopioitujen tunnusten hyödyntämistä. Esimerkiksi logistiikan käytössä olevassa EPC-järjestelmässä kaikki tunnistekoodit on syötetty maailmanlaajuiseen tietopankkiin, josta tunnistekoodin tarkastuksella voidaan estää olemattomien ja kloonattujen tunnistekoodien käyttö. (IZT, Empa & BSI, 2004.)

Hyvin usein todennuksessa voidaan käyttää challenge-response-järjestelmää, jossa lukulaite lähettää sattumanvaraisesti tuotetun numerosarjan tai sisäisen kellon ajan, mistä tunnisteen täytyy lähettää takaisin oikealla lailla salattu tai muunneltu vastaus. Challenge-response-järjestelmä on määritelty RFID-tekniikkaan pohjautuville laitteille ISO 9798 -standardissa. Oleellisimpina turvaominaisuuksina on tässä tapauksessa käytetty ennalta valittua salaustapaa, jota ei kuitenkaan lähetetä lukulaitteelta missään vaiheessa. Toisena turvaominaisuutena toimii tunnisteen ja lukulaitteen välisen tiedonsiirron salakuuntelun ja toistamisen mahdottomuus, koska käytetty sattumanvarainen numerosarja on jo vaihtunut. (IZT, Empa & BSI 2004.)

Salausavaimen fyysinen lukeminen tunnisteelta on mahdollista, mutta se vaatii tarkoitukseen sopivan laboratoriolaitteiston, jolla voidaan mikroprosessori fyysisesti kuoria kerros kerrokselta. Kuoritut kerrokset voidaan tällöin analysoida mikroskooppisesti. (IZT, Empa & BSI, 2004.)

Edellä mainittua salausavaimen lukemistapaa hyödynnettiin MiFare Classic -mikroprosessorin salauksen murtamisessa vuonna 2008 (Dayal, 2008).

RFID-tekniikkaa hyödyntävissä järjestelmissä todennuksesta voidaan tehdä teoreettisesti mahdoton murtaa, mutta sen vaatimat ominaisuudet niin tunnisteelta, lukijalta kuin hallintajärjestelmältä ovat erittäin suuret. Suuret ominaisuusvaati-

mukset tarkoittavat, että tarvitaan tehokkaampi ja kalliimpi mikroprosessori. (IZT, Empa & BSI 2004.)

3.1.2 Salaus

Tietoliikenteen salauksessa on tarkoituksena, että sekä lähetettävä että vastaanotettava tieto on salattua. Salatun tiedon lukeminen onnistuu hyödyntämällä salausavainta, joka voi olla ennalta määrätty tai voidaan luoda tapauskohtaisesti hyödyntämällä edellä mainittua challenge-respose-järjestelmää. Normaalisti vahvaa salausta hyödyntävissä järjestelmissä hyödynnetään myös vahvaa todennusta. (IZT, Empa & BSI, 2004.)

Yleisimmin hyödynnetty salaustapa pohjautuu epäsymmetriseen salaukseen, jossa hyödynnetään kahta erilaista salausavainta. Salausavaimet ovat matemaattisesti linkitetty, mutta niitä ei voida käytännössä laskea toisistaan. Salauksessa toinen avain salaa tiedon ja toisella tieto voidaan purkaa. (Shepard 2004, 126.)

Tunnisteissa, jotka sisältävät vain tunnistekoodin, ei tunnisteen luvaton lukeminen aiheuta todennäköisesti suuria vahinkoja, mutta tunnisteissa, jotka sisältävät tärkeää tietoa, kuten esimerkiksi lähimaksukortin maksukorttitiedot, olisi vahva salaus paras suoja luvattoman lukemisen estämiseksi. Tällöin tarvittaisiin jällen tehokkaampi mikroprosessori. (IZT, Empa & BSI 2004.)

3.1.3 Pseudonymisaatio

Pseudonymisaatiolla tarkoitetaan uuden salauksen generoimista jokaiselle lukukerralle. Ero edellä mainittuihin tekniikoihin tulee siitä, että uusi salaus tai meta-id, eli tunnisteen muunneltu tunnistekoodi, tuotetaan tunnisteen toimesta. (IZT, Empa & BSI, 2004.)

Tarkoituksena on tuottaa jokaisen lukutapahtuman jälkeen tunnisteelle uusi meta-id, eli väliaikainen tunniste, joka luodaan sattumanvaraisesta numerosarjasta ja todellisesta tunnistekoodista. Tuotettu meta-id ja sen tuottamiseen käytetty sattumanvarainen numerosarja lähetetään tämän jälkeen lukijalle, joka puolestaan lä-

hettää sen hallintajärjestelmälle. Hallintajärjestelmän käsittelee tämän jälkeen kaikki rekisterissä olevat tunnistekoodit saamallaan sattumanvaraisella numerosarjalla, kunnes vastaava löytyy ja tunniste voidaan varmentaa. (IZT, Empa & BSI 2004.)

Suuren tunnisterekisterin kanssa pseudonymisaatio ei ole kovin käytännöllinen. Muihin tietoturvaratkaisuihin verraten se vaatii kuitenkin vähinten itse tunnisteilta, joten se voidaan ottaa käyttöön melko kustannustehokkaasti. Ainoa vaatimus tunnisteilta on että mikroprosessori pystyy tuottamaan sattumanvaraisia lukuja. (IZT, Empa & BSI 2004.)

Pseudonymisaatio voidaan viedä pidemmälle tuottamalla samasta tunnistekoodista ensin yksi meta-id ja sen jälkeen ensimmäisestä meta-id:stä luodaan vielä toinen meta-id, joka puolestaan lähetetään lukijalle ja hallintajärjestelmälle. Teoreettisesti tätä meta-id:n linkitystä voidaan tehdä useita kertoja, mutta sen vaatimukset lukijalle ja hallintajärjestelmälle kasvavat. (IZT, Empa & BSI 2004.)

3.1.4 Lukemisen estäminen

Normaalisti RFID- ja NFC-tunnisteissa ei ole varsinaista ON/OFF-kytkintä ja tunniste on jatkuvasti valmis lähettämään sisältämäänsä dataa eteenpäin huolimatta siitä onko sisältö suojattua vai ei. Tästä johtuen voidaan tunnisteissa olevaa dataa helposti lukea käyttäjien sitä huomaamatta. (IZT, Empa & BSI 2004.)

Yhdysvalloissa Pittsburgin yliopistossa on kuitenkin kehitetty RFID- ja NFC-tunnisteille ON/OFF-kytkin. Vuonna 2012 julkistetussa patenttihakemuksessa esitellään erityisesti lähimaksukorteissa hyödynnettävä kytkin, joka aktivoituu kun kortista pidetään tietystä kohtaa kiinni ja sammuu kun kortista päästetään irti. (Biddle 2012.)

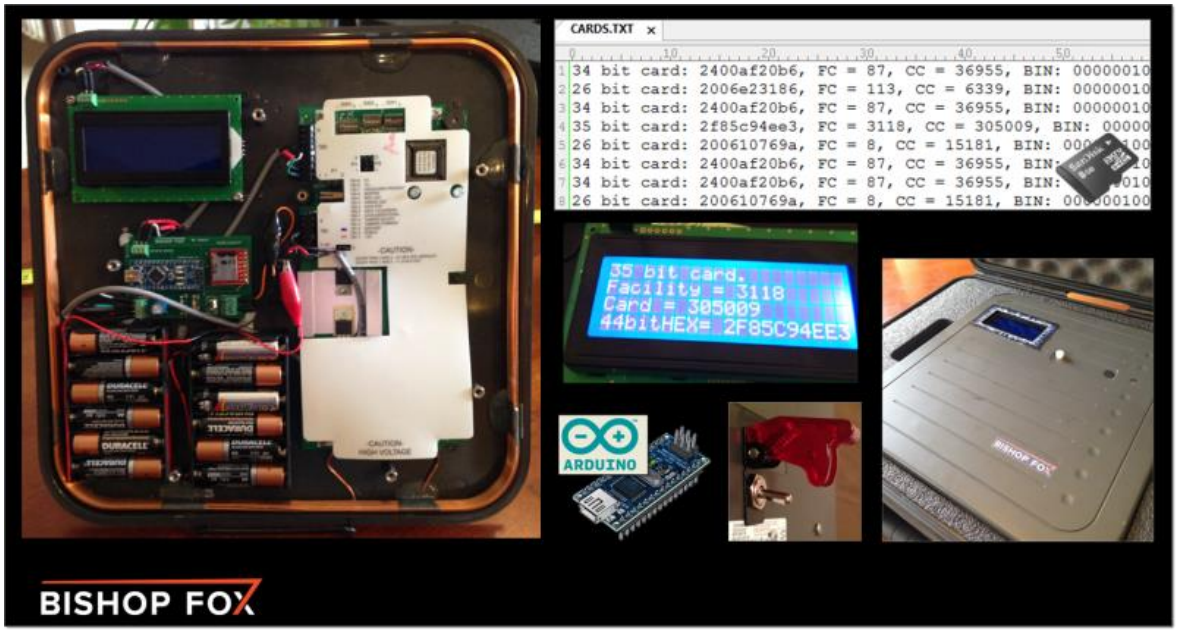
3.2 Tunnisteen luvaton lukeminen

Valmistajien ja palveluntarjoajien käytettävissä olevat turvatoimet tunnisteiden ja tiedonsiirron turvaamiseksi on esitelty edettävissä kappaleissa. Esitetyillä turva-

toimilla pystyttäisiin kasvattamaan käytettävien RFID- ja NFC-järjestelmien tietoturvaa, mutta myös järjestelmien kustannukset kasvavat. Kustannussyistä on hyvin yleistä, että esimerkiksi kulunvalvonnan tehtävissä käytettävät tunnukset eivät välttämättä sisällä minkäänlaista todennus- tai salausjärjestelmää. Tällä tarkoitetaan sitä, että jos tunniste aktivoidaan järjestelmään kuulumattomalla lukijalla, lähettää tunniste sisältämänsä tunnistekoodin selkokielisenä eli sitä ei ole salattu tai suojattu. (Brown, 2013.)

Tunnisteen varsinainen kuuntelu voidaan toteuttaa esimerkiksi niin sanotulla a$$ grabbing-metodilla, jossa luvattoman lukulaitteen omaava henkilö tuo lukulaitteen erittäin lähelle kohteena olevaa tunnistetta. Uusien kehittyneempien välineiden avulla voidaan tunnisteita lukea huomattavankin matkan päästä. Käytettävien laitteiden koot ovat myös pienentyneet tekniikan kehittyessä. (Brown 2013.)

Bishop Fox -turvakonsulttiyhtiö on julkaissut ohjeet pitkän lukuetäisyyden RFID-lukijan rakentamiseen. Tastic RFID Thief -laitteen pohjana käytetään yleisesti saatavilla olevia RFID-lukulaitteita, joihin liitetään Arduinon mikrokontrolleri. Mikrokontrolleri voidaan liittää melkein kaikkiin kaupallisesti saatavilla oleviin lukijoihin. (Bishop Fox 2013.) Kuviosta 23 voidaan nähdä Tastic RFID Thief -laite yhdistettynä lukijaan.



Kuvio 23. Tastic RFID Thief (Brown 2013)

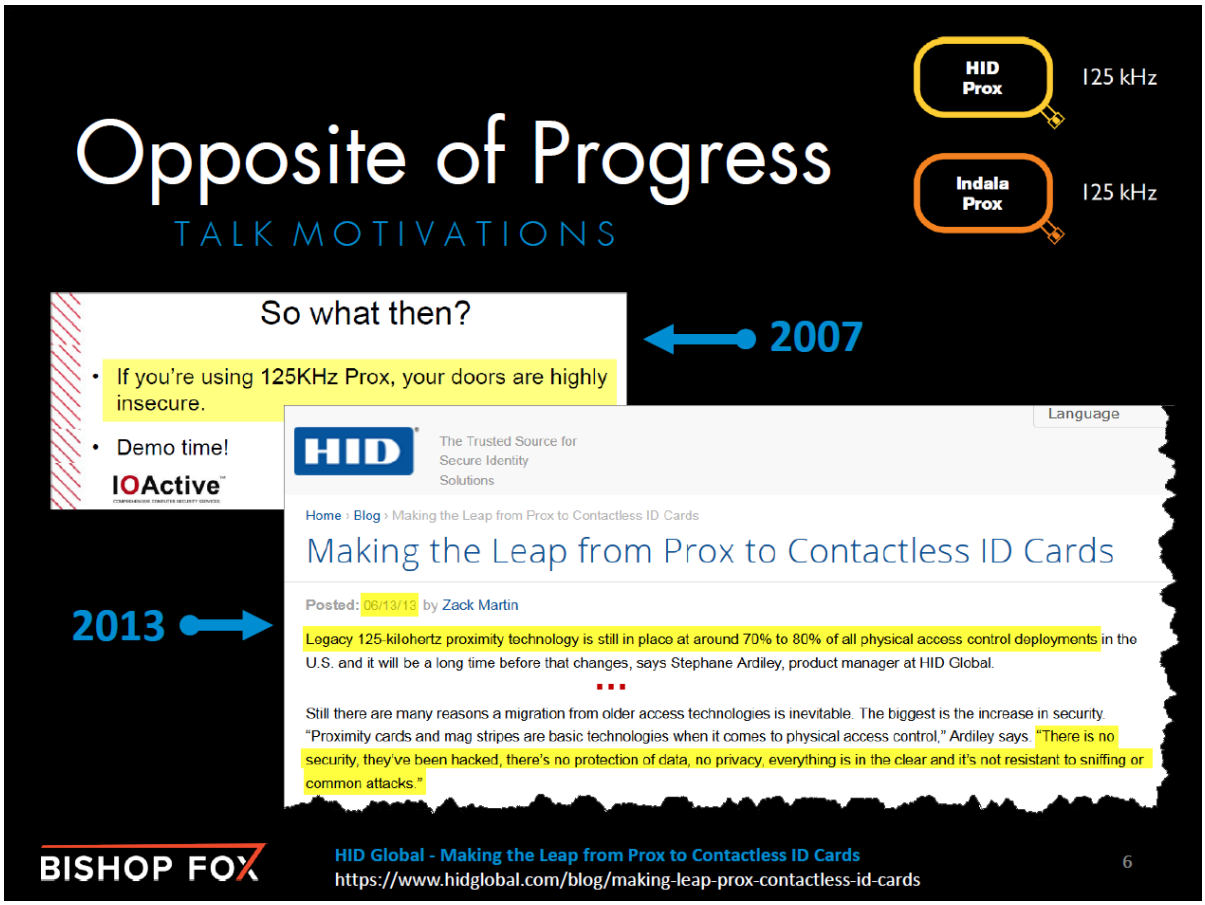
3.3 Tunnisteen murtaminen

Tunnisteen murtamisella tarkoitetaan tunnisteen sisältämän salatun datan muuttamista luettavaan muotoon.

Useiden RFID-valmistajien tunnisteiden salauksia on onnistuttu purkamaan, mikä on lisännyt tarvetta korostaa RFID-johdannaisten järjestelmien ja laitteiden tietoturvaa. Yksi tunnetuimmista salauksista on vuonna 2008 tapahtunut NXP Semiconductors -valmistajan Mifare Classic -mikroprosessoria hyödyntävien tunnisteiden salauksen purkaminen. Kyseistä mikroprosessori hyödynnettiin laajalti monissa eri sovelluksissa ja järjestelmissä. Valmistajan kompastuskivenä oli, ettei mikroprosessorin salausteknologiaa oltu parannettu sitten sen julkistamisen vuonna 1994, jolloin käytetty 48-bittinen salaus oli vielä huippuluokkaa. (Gaudi 2008.)

Kesäkuussa 2013 Stephany Ardillry, HID Global -yhtiön tuotepäällikkö ilmoitti, sittemmin poistetussa, yritysblogissaan kuinka Legacy 125kHz -sarjan tuotteet on kaikki murrettu ja käyttäjillä ei ole käytännössä enää minkäänlaista suojausta luvatonta käyttöä vastaan. Samassa blogissa Ardiley vielä huomauttaa kuinka Yhdysvalloissa käytössä olevista kulunvalvontajärjestelmistä 70–80 prosenttia yhä käyttää kyseistä teknologiaa. (Ardilly, 2013, Brownin mukaan.) Kuviosta 24 voidaan nähdä julkaisuja koskien Legacy 125kHz -sarjan tietoturvaa.

Kyseisen Legacy 125kHz -sarjan tuotteet todistettiin erittäin haavoittuvaisiksi jo vuonna 2007 (Paget, 2007).



Kuvio 24. 125 kHz:n murtaminen (Brown, 2013)

3.4 Tunnisteen luvaton kopiointi

Tunnisteen luvattomalla kopioinnilla tarkoitetaan käytössä olevan tunnisteen sisältämän datan siirtämistä toiselle tunnisteelle. Tätä toimintoa edeltävät normaalisti tunnisteen luvaton kuuntelu ja murtaminen.

Francis Brown, Bishop Fox -turvakonsulttiyhtiön edustaja, esitteli Black Hat USA 2013 -tapahtumassa kuinka helposti olemassa olevia RFID-järjestelmiä on mahdollista lukea, murtaa ja kopioida. Pääsyyksi hän esittää järjestelmien 20-vuotisen elinkaaren, josta johtuen laitteiden tietoturvan taso ei vastaa nykyvaatimusten tasoa. (Brown 2013.)

3.5 Lukulaitteen elektroninen kiertäminen

Lukulaitteen elektronisella kiertämisellä tarkoitetaan kohteena olevan lukulaitteen ja siihen kytkettyjen järjestelmien hyödyntämistä ilman tunnisteita.

Suurin osa olemassa olevista turvajärjestelmien lukulaitteista käyttää tai voi käyttää Wiegand-protokollan mukaista tiedonsiirtotapaa lukijan ja hallintajärjestelmän välillä. Kyseinen protokolla ei ole ainoa käytettävä tiedonsiirtotapa, mutta suurin osa erilaisista lukijoista ja hallintajärjestelmistä käyttää sitä. (Franken 2008.)

On mahdollista kytkeytyä suoraan lukulaitteen mikroprosessorille tai jopa asentaa koteloinnin sisälle oma elektroninen laitteisto olemassa olevien komponenttien päälle. Tällainen laite on esimerkiksi Zac Frankenin vuonna 2007 esittelemä Gecko, joka asennetaan joko lukijan sisälle tai lukijasta lähteviin johtoihin. Gecko tallentaa asennuksen jälkeen tapahtuvia lukutapahtumia ja pystyy tarvittaessa toistamaan niitä uudelleen. Koska lukulaitteiden ja hallintajärjestelmän välinen tiedonsiirto on normaalisti salaamatonta ja noudattaa Wiegand-protokollaa, ei laitteen käyttö rajoitu RFID-lukijoihin vaan sitä voidaan hyödyntää kaikissa kulunvalvontalaitteistoissa, joissa lukijoita ei ole suojattu sabotaasikytkimillä tai vastaavilla turvaominaisuuksilla. Suurinta osaa kulunvalvonnassa käytetyistä lukijoista ei ole suojattu millään lailla koteloinnin luvatonta avaamista vastaan. Frankenin mukaan Wiegand-protokollaa ei voida vain päivittää paremmaksi, se tulisi kokonaisuudessaan vaihtaa toimivampaan ratkaisuun. (Zetter 2008.) Kuviossa 25 voidaan nähdä Frank Zetterin Gecko.

Kuvio 25. Gecko yhdistettynä RFID-lukijaan (Zetter 2007)

3.6 Lähimaksukorttien hyödyntäminen

Suomessa NFC-teknologiaan pohjautuvia lähimaksukortteja tarjoavat muun muassa Danske Bank, OP-Pohjola ja Nordea. Kyseisten kolmen palveluntarjoajan kesken lähimaksutoiminnon omaavia kortteja oli joulukuussa 2014 liikenteessä lähes miljoona kappaletta eli joka viidennellä suomalaisella oli käytössään lähimaksukortti. (HS 2014.)

Lähimaksukorttien määrän voidaan olettaa vain kohoavan varsinkin kun useat pankit ovat lisäämässä lähimaksuominaisuuden pakolliseksi maksukortteihin. Esimerkiksi OP-Pohjola ja Nordea lähettävät korttikannan uusinnan yhteydessä kortin, jossa on lähimaksuominaisuus. (Kalmi 2013.)

Yksi lähimaksukorttien yleistymisen pääsyistä on korotettu tietoturva ja maksamisen nopeutuminen alle 25 euron ostoksissa. Korotetulla tietoturvalla tarkoitetaan, että käyttäjän ei tarvitse enää syöttää PIN-koodiaan, jolloin kukaan ei sitä voi nähdä. Kuitenkin ensimmäistä kertaa lähimaksuominaisuutta käyttäessä tulee PIN-

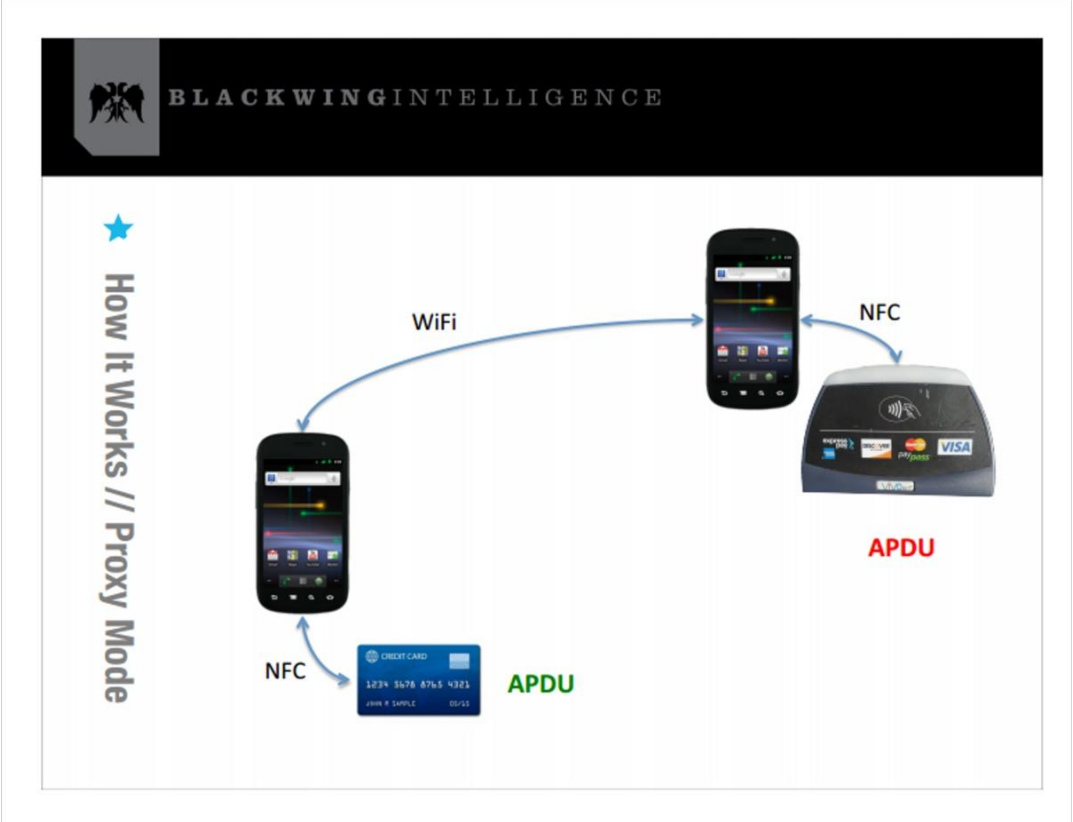
koodi syöttää sekä tiettyjen käyttökertojen jälkeen. (OP, [Viitattu: 31.3.2015];Nordea, [Viitattu:31.3.2015].)

Erityisesti on huomioitava, että lähimaksuominaisuuden tuoma tietoturva vaikeuttaa maksukortin fyysistä varastamista, mutta tekee maksukortin sisältämien tietojen varastamisesta huomattavasti helpompaa. Suomalainen kyberturvallisuus yritys Nixu testasi toukokuussa 2013 onko mahdollista lukea lähimaksukorteilta tietoa. Kokeilun tuloksena oli, että noin 20 euron lukulaitteella ja alle sekunnissa oli lähimaksuominaisuuden omaavalta kortilta luettu maksukorttinumero, voimassaoloaika ja kortinhaltijan nimi. Kyseessä on siis täysin suojaamatonta tietoa, jonka kuka tahansa oikeanlaisen lukulaitteen omaava henkilö voisi saada tietoonsa. Kyseisen testauksen lisäksi selvitettiin, että kyseisillä tiedoilla voitiin ostaa nimeltä mainitsemattoman suuren kansainvälisen verkkokaupan sivuilta ostoksia. Verkkoostoksissa lähimaksukortin 25 euron maksurajoitusta ei oteta huomioon, jolloin rahallinen hyöty rikollisesta hyödyntämisestä voi olla erittäin suuri. (Nixu 2013.)

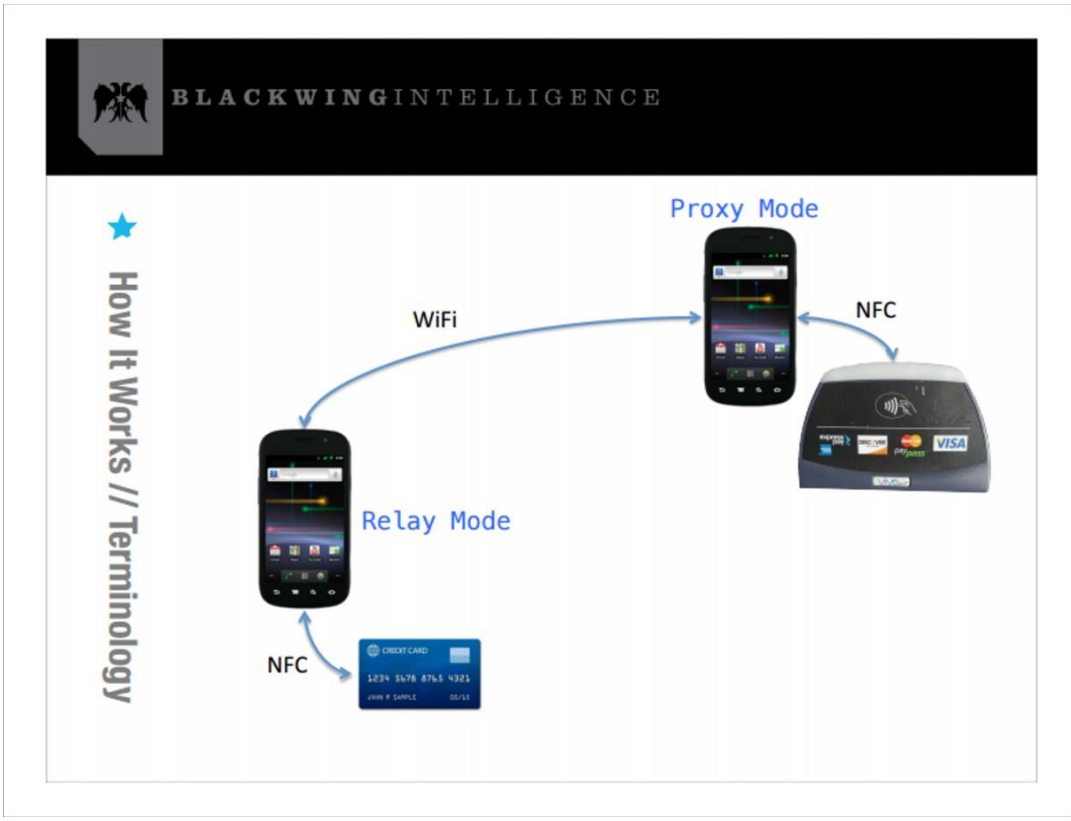
Kyseinen tietoturva-aukko ei ole uusi asia, sillä jo vuonna 2006 esitellyssä tutkimuksessa todistettiin, että ensimmäisen sukupolven lähimaksukorteista löydettiin samat haavoittuvuudet kuin Nixun tekemässä vuoden 2013 testissä. Valmistajat suunnittelivat kohottavansa turvatoimia jo vuonna 2006 seuraavan sukupolven lähimaksukortteihin poistamalla korteista lähetettävästä datasta kortin haltijan nimen. (Schwartz 2006.)

Yksi hienostuneimmista ja uusimmista lähimaksukorttien tietoja kaappaavasta ja hyödyntävästä laitteistosta on vuonna 2014 Eddie Leen kehittelemä laitteistokokonaisuus, jossa kahden NFC-tekniikkaa hyödyntävän puhelimen avulla voidaan suorittaa veloituksia lähimaksukortilta. Yksinkertaisimmassa esimerkissä NFC-lukutilassa oleva matkapuhelin tuodaan lähimaksukortin läheisyyteen, joka kerää tarvittavaa tietoa kortilla. Samaan aikaan toisella matkapuhelimella emuloidaan lähimaksukorttia hyödyntäen NFC-toimintoa sen samalla ollessa maksupäätteen läheisyydessä. Maksupääte lähettää emuloivalle matkapuhelimelle APDU-pyynnön, joka lähetetään langattoman internetyhteyden kautta lukutilassa olevalle matkapuhelimelle. Tällöin lähimaksukortti vastaa APDU-pyyntöön lähettämällä oikeanlaisen datan takaisin ja maksu saadaan suoritettua maksupäätteellä. Järjestelmällä voidaan myös analysoida matkapuhelinten välillä tapahtunut tietoliikenne

ja täten purkaa ja toistaa maksukortin tiedot. (Lee 2012.) Kuvioissa 26 ja 27 esitellään Leen laitteiston tietoliikenneväylät ja tilatoiminnot.

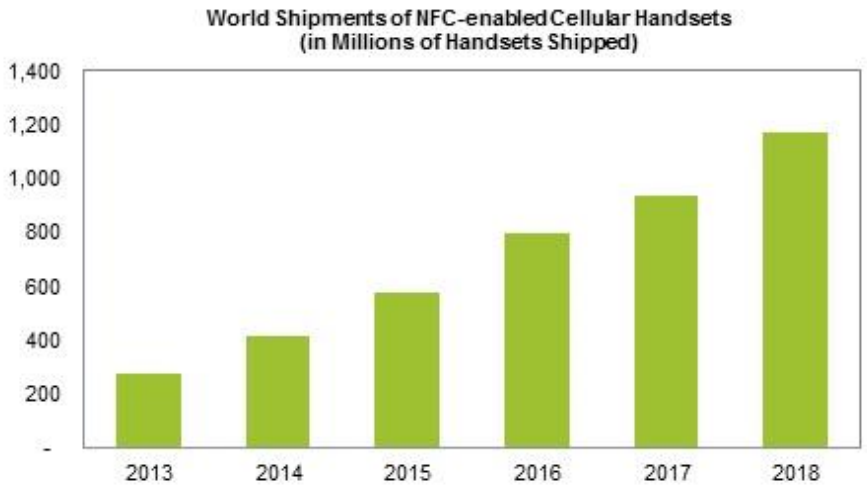


Kuvio 26. Leen laitteiston tietoliikenneväylät (Lee 2012.)



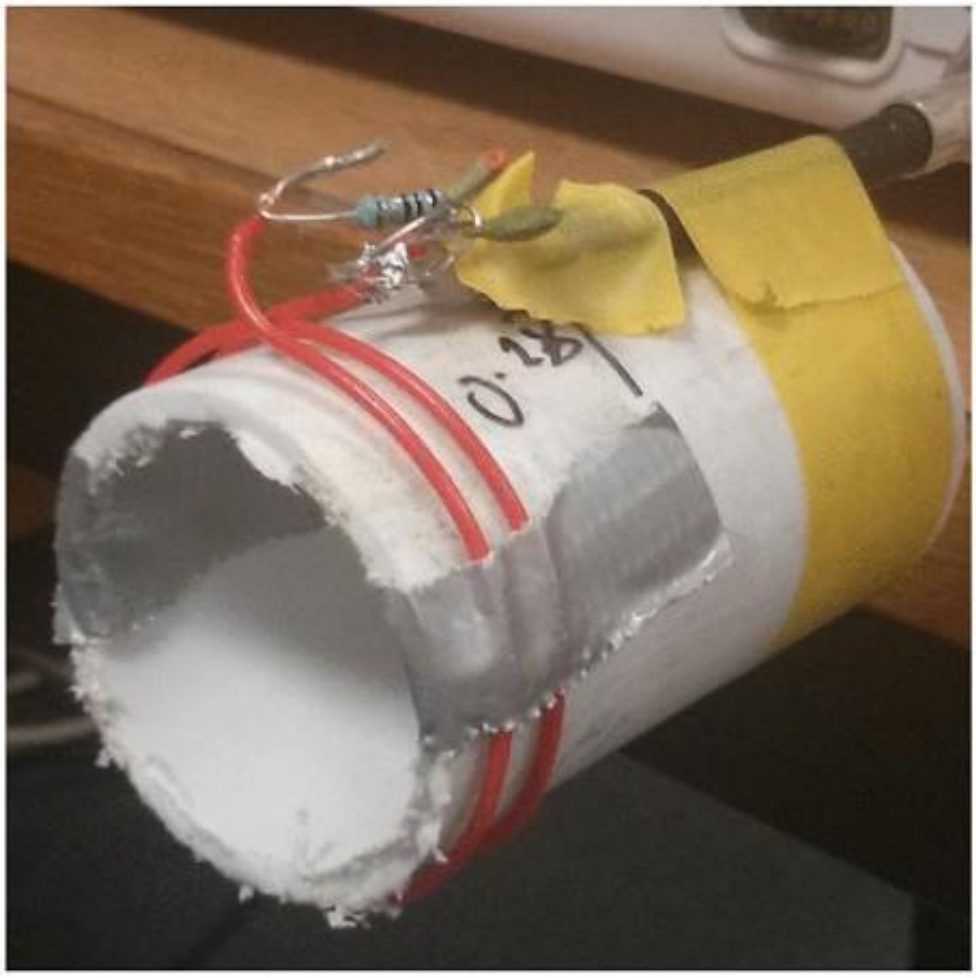
Kuvio 27. Leen laitteiston tilatoiminnot (Lee 2012.)

IHS Technologyn julkaisemassa tutkimuksessa esitellään, kuinka NFC:n hyödyntäminen matkapuhelimissa lisääntyy huomattavasti vuoteen 2018 mennessä. Vuonna 2012 toimitetuista 1,5 miljardista matkapuhelimesta 18,2 % hyödynsi NFC-tekniikkaa ja vuoteen 2018 mennessä määrä nousee 64 %. (Tait 2014.) Kuviosta 28 voidaan nähdä NFC-matkapuhelinten toimitusmäärät.



Kuvio 28. NFC-matkapuhelinten toimitusmäärät vuosina 2013–2018 (Tait 2014)

Yksi suurimmista mainostetuista tietoturvaominaisuuksista lähimaksukorteissa on lyhyt lukuetäisyys. Useissa yhteyksissä on tullut ilmi, että lähimaksukorttien lukeminen tarkoitettua pidemmältä etäisyydeltä on mahdollista, mutta tarvittava erikoislaitteisto on erittäin kallis. Surreyn yliopiston tutkimusryhmä on kuitenkin kehittänyt mobiilin, halvan ja helposti piilotettavan laitteiston lähimaksukorttien lukemiseen mainostettua suurinta lukuetäisyyttä pidemmiltä etäisyyksiltä. Laitteistolla onnistuttiin lukemaan lähimaksukorttien sisältämää tietoa 45–80 senttimetrin päästä. (Diakos, Briffa, Brown & Wesemeyer 2013.) Kuviosta 29 voidaan nähdä laitteistossa käytetty erittäin yksinkertainen kela-antenni.



Kuvio 29. Surreyn yliopiston tutkimustyhmän laitteistossa käytetty kela-antenni (Diakos, Briffa, Brown & Wesemeyer 2013)

4 LOPPUPÄÄTELMÄT

Tässä opinnäytetyössä esitellyillä tietoturvaratkaisuilla olisi mahdollista valmistaa täysin tietoturvallisia kulunvalvonnan ja lähimaksun sovelluksia. Hyvin usein kyseisten sovellusten tietoturva on kaukana siitä, mitä se voisi parhaimmillaan olla.

Kulunvalvontajärjestelmissä tietoturvan tasoon vaikuttaa useampi asia kuin pelkästään tietoturva. Kulunvalvonnassa laitteistojen ikä ratkaisee myös hyvin paljon. Suurin osa kulunvalvonnan laiteperäisistä ongelmista pohjautuu juuri laitteiden erittäin pitkään käyttöikään. Nykyaikaisten tietoturvaratkaisujen implementointi vanhoihin laitteistoihin on hyvin usein erittäin vaikeaa, ja usein ainoana ratkaisuna on uuden järjestelmän asentaminen. Kuitenkin samat ongelmat löytyvät useista uusistakin järjestelmistä, jolloin voidaan vain olettaa että laitteiston ikä ei kuitenkaan ole tietoturvan heikkouden ainoa perusta, vaan ongelmat pohjautuvat myös laitteiden valmistuskustannuksiin ja hintoihin. Kun pyritään tuottamaan edullisia tuotteita, joudutaan usein tinkimään laadusta. Tässä tapauksessa RFID-tekniikkaan pohjautuvissa kulunvalvontajärjestelmissä kärsii eniten tietoturva, kun edullisesti tuotetuilla laitteilla ei voida tuottaa tehokasta todennusta tai salausta.

Tästä johtuu, että tällä hetkellä käytössä olevien RFID-järjestelmien tietoturva on riittämätön. Tämä koskee suurinta osaa käytössä olevista laitteista ja järjestelmistä, joiden käyttöikä on selvästi pidempi kuin laitteille suunnitellun tietoturvan voidaan ikinä olettaa olevan. Tämä ei kuitenkaan tarkoita että laitteisto olisi täysin turvaton. Jos edes laitteiden käyttäjät eivät tiedä mitä tekniikkaa laitteet hyödyntävät ja kuinka, voidaan olettaa että on olemassa aina jonkin asteinen tietoturva, joka ei perustu millään lailla tekniikkaan, vaan pohjautuu ihmisten tietämättömyyteen. Tätä voidaan verrata henkilöön joka osaa käyttää normaalia avainta oven avaamiseen, muttei tiedä kuitenkaan mitä tämä avain tekee lukon sisällä. Toisaalta taas henkilö joka tietää kuinka lukko toimii voi hyödyntää tietämystään lukon avaamiseen ilman avainta.

Olemassa olevien järjestelmien tietoturva on riittämätön, mutta tämä ei tarkoita ettei olisi olemassa järjestelmiä, joissa tietoturva on hyvä. Ongelmat alkavat, kun pyritään tuottamaan taloudellisesti halpoja ratkaisuja, joiden implementointi olemassa oleviin järjestelmiin olisi mahdollisimman helppoa. Tämä kuulostaa hyvältä

asialta ja osittain se onkin, mutta tämä johtaa myös siihen että halvalla ei saada tarpeeksi hyvää tietoturvaa aikaiseksi, ja jos implementointi vanhoihin järjestelmiin on helppoa, tuo se tullessaan myös osan vanhojen järjestelmien tietoturva-aukoista.

RFID-tekniikkaa hyödyntävien kulunvalvontajärjestelmien turvallisuutta tukevat kuitenkin sekundaariset turvalaitteet, kuten turvakamerat, liiketunnistimet ja erilaiset muut ilmaisimet. Nykyisten käytössä olevien RFID-kulunvalvontajärjestelmien käyttäminen ilman sekundaarisia turvalaitteita olisi asiaan perehtyneelle henkilölle lähinnä vain vitsi, mutta onneksi turva-alan ammattilaiset ymmärtävät olla luottamatta vain yhteen kohteen suojaustapaan. Ikävä kyllä markkinoilla on olemassa erityisesti kotitalouksille suunnattuja hälytinjärjestelmiä, jotka käyttäjä voi kytkeä pois päältä RFID-tunnisteella. Kyseinen tunniste voidaan helposti kopioida, jolloin tunnisteen kopioinut osapuoli, luvallinen tai luvaton, pystyy sammuttamaan hälytinjärjestelmän. Tämä kertoo kuinka helppous ja turvallisuus eivät todellakaan aina kulje käsi kädessä.

Lähimaksukorttien tietoturva on myös riittämätön, osittain jopa huonompi kuin vanhojen RFID-järjestelmien. Tässä opinnäytetyössä esiteltiin esimerkkitapauksia, kuinka lähimaksukortilta voidaan lukea helposti tietoa ja tämän jälkeen hyödyntää tätä tietoa. Esiteltiin kuinka NFC-matkapuhelimet ovat yleistymässä maailmanlaajuisesti sekä lisäksi kerrottiin lähimaksukorttien hyödyntämästä datarakenteesta, joka on vapaasti saatavilla. Yhdessä nämä muodostavat erittäin pahan ongelman lähimaksukorttien tietoturvalle. RFID-järjestelmiä murtaessa tarvittiin sentään erikoislaitteita, mutta pian ihmisten käyttämistä matkapuhelimista kaksi kolmesta sisältää NFC-ominaisuuden, jolla voidaan lukea lähimaksukortteja. Lisäksi lukemiseen ei tarvita edes erityistä osaamista tai vaivaa kun lukuohjelmat ovat vapaasti ja laillisesti ladattavissa erinäisistä sovelluskaupoista. Koska lähimaksukortilta voidaan lukea tiedot sähköisesti, ei kortin omistaja saa välttämättä koskaan tietää että lähimaksukortin tiedot on varastettu. Lähimaksukorteista pystytään tekemään turvallisia, mutta nykytilassaan ne ovat äärimmäisen alttiita väärinkäytöksille.

Lähimaksukorttien hyödyksi mainostetaan maksutapahtuman nopeutta ja turvallisuutta. NFC-tiedonsiirrolla saadaan todella aikaan nopeampi kassatapahtuma, mikä on varmasti myös asiakkaan mielestä kätevä, mutta samalla saadaan aikaan

turvaton maksukortti. Monessa eri lähteessä, suomalainen Nixu-tietoturvayhtiö mukaan luettuna, on todettu että korteilta voidaan helposti lukea tietoa. Kuitenkin jokaisessa lähimaksukortteja tarjoavassa pankissa korostetaan kuinka turvallinen kortti on. Turvallisuudella tarkoitetaan tässä tapauksessa tietenkin sitä, kuinka lähimaksukorttia käyttäessä ei tarvitse aivan niin usein syöttää PIN-koodia maksupäätteelle. Loppujen lopuksi kaikki laittomista lähimaksukorttien hyödyntämisestä koostuvat kustannukset päätyvät pankkien ja sitä kautta vakuutusyhtiöiden korvattavaksi. Tämä kuitenkin vaatii sen, että lähimaksukortin haltija tarkkailee jopa päivittäin tilitapahtumiaan ja pystyy tunnistamaan virheelliset maksutapahtumat. Voidaan olettaa, että pienien rahasummien maksutapahtumia ei vaivauduta edes tarkastamaan tarkemmin.

RFID-kulunvalvontajärjestelmät ja lähimaksukortit käyttävät tällä hetkellä riittämätöntä tietoturvaa, mutta niistä voidaan tehdä turvallisia. Kulunvalvontajärjestelmistä on olemassa jo tällä hetkellä järjestelmiä, joiden tietoturva on riittävä, mutta kyseiset järjestelmät ovat kustannuksiltaan korkeammat. Kuluttajat suosivat kuitenkin kustannuksiltaan alhaisia järjestelmiä, jolloin myös tietoturvan taso on huomattavasti alempi. Lähimaksukorttien käyttöönotosta vastaavat pankit, jolloin myös uuden korttikannan implementoinnissa on pyritty toimimaan kustannustehokkaasti.

Maailmanlaajuisella tasolla lähimaksukorttien käyttöönotosta on pyritty tekemään mahdollisimman helppoa, mikä on osittain aiheuttanut myös niiden tietoturvan huonon tilan. Implementoinnin helppoudella tarkoitetaan että lähimaksukortti ei sisällä uusia turvaominaisuuksia, vaan hyödyntää vanhoja sirukortillisten maksukorttien turvaominaisuuksia, joissa ei oteta huomioon langatonta tietoliikennettä lähimaksukortin ja maksuterminaalin välillä.

Yksinkertaista, nopeaa ja halpaa ratkaisua kyseisiin tietoturvaongelmiin ei ole. Tehokkaammat salaukset ja todennukset vaativat tehokkaampia laitteita, jotka puolestaan ovat kustannuksiltaan korkeammat. Joissain tapauksissa voidaan tietoturvaa kohottaa eriyttämällä järjestelmiä nykystandardeista ja suunnitella uutta, mutta tällöin laitteiden implementointi vanhoihin järjestelmiin vaikeutuu ja laitteiden maailmanlaajuinen käyttöönotto saattaa jäädä vain haaveeksi. Todennäköisesti kuluu vielä vuosia ennen kuin järjestelmät alkavat muuttua.

LÄHTEET

Seppä, H. 2011. RFID-etätunnistus - mahdollisuudet ja uhat. [Verkkojulkaisu]. Eduskunnan tulevaisuusvaliokunta. Helsinki. [Viitattu 9.2011]. Saatavissa: http://web.eduskunta.fi/dman/Document.phx?documentId=xh18211145145785&cmd=download

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Porvoo: WSOY.

Miles, S., Sarma, S. & Williams, J. 2008. RFID Technology and Applications. Cambridge: Cambridge University Press.

Shepard S. 2005. RFID Radio Frequency Identification. McGraw-Hill.

Roberti, M. 2005. The History of RFID Technology. [Verkkojulkaisu]. RFID Journal LLC. [Viitattu 24.3.2015]. Saatavissa: http://www.rfidjournal.com/articles/pdf?1338

Finkenzeller, K. 2003. RFID Handbook. 2.p.,uud. p. West Sussex: Wiley.

CNRFID. Ei päiväystä. RFID frequency spectrum. [verkkosivu]. French National RFID Center. [Viitattu 24.3. 2015]. Saatavissa: http://www.centrenational-rfid.com/rfid-frequency-ranges-article-16-gb-ruid-202.html

Violino, B. 2005. RFID Business Applications. [Verkkojulkaisu]. RFID Journal LLC. [Viitattu 24.3.2015]. Saatavissa: http://www.rfidjournal.com/articles/pdf?1334

Poole, I. Ei päiväystä. NFC Near Field Communication Tutorial. [verkkosivu]. Adrio Communications Ltd. [Viitattu 24.3.2015]. Saatavissa: http://www.radio-electronics.com/info/wireless/nfc/near-field-communications-tutorial.php

Impinj. Ei päiväystä. RFID Standards. [www-dokumentti]. Impinj Inc. [Viitattu 25.3.2015]. Saatavissa: http://www.impinj.com/resources/about-rfid/rfid-standards/

EMVCo. Ei päiväystä. EMV Contactless Specifications for Payment Systems; Book A: Architecture and General Requirements. [Verkkojulkaisu]. EMVCo LLC. [Viitattu 25.3.2015]. Saatavissa: http://www.emvco.com/specifications.aspx?id=21

NFC Forum. Ei päiväystä. Our Mission & Goals. [verkkosivu]. NFC Forum. [Viitattu 25.3.2015]. Saatavissa: http://nfc-forum.org/about-us/the-nfc-forum/

Bonsor, K. & Fenlon, W. 2007. How RFID Works. [verkkosivu]. InfoSpace LLC. [Viitattu 26.3.2015]. Saatavissa: http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid.htm

HID Global. Ei päiväystä. FlexKey Keytag. [verkkosivu]. HID Global Corporation/ASSA ABLOY AB.[Viitattu 26.3.2015]. Saatavissa: http://www.hidglobal.com/products/cards-and-credentials/indala/flexkey-keytag

BBC. 2007. World's tiniest RFID tag unveiled. [verkkosivu]. Brittish Broadcasting Corporation. [Viitattu 26.3.2015]. Saatavissa: http://news.bbc.co.uk/2/hi/technology/6389581.stm

CISCO. 2008. Enterprise Mobility 4.1 Desing Guide; Chapter 6: RFID Tag Considerations. [Verkkojulkaisu]. CISCO Systems Inc. [Viitattu 26.3.2015]. Saatavissa: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.pdf

Cadamuro, M. 2011. CAEN EFID is offering Gen 2 semi-passive RFID tags and development kits for cold chain monitoring applications. [verkkosivu]. Veryfields. [Viitattu 26.3.2015]. Saatavissa: http://www.veryfields.net/caen-rfid-offers-semi-passive-gen-2-rfid-tags-and-development-kits-for-cold-chain-monitoring-applications

Chandler, N. 2012. What's an NFC tag? [verkkosivu]. InfoSpace LLC. [Viitattu 26.3.2015]. Saatavissa: http://electronics.howstuffworks.com/nfc-tag1.htm

Arnall, T. 2007. RFID tags. [verkkosivu]. Yahoo! Inc. [Viitattu 26.3.2015]. Saatavissa: https://www.flickr.com/photos/timo/1616057288/in/photostream/

Minto, R. 2014. Disabling contactless payment cards, or preventing "card clash" with Oyster. [verkkosivu]. Robin Minto. [Viitattu 26.3.2015]. Saatavissa: http://robinminto.com/blog/post/2014/03/21/Disabling-contactless-payment-cards-or-preventing-card-clash-with-Oyster

TutorialsWeb. Ei päiväystä. RFID (Radio Frequency Identification): A Tutorial. [verkkosivu]. TutorialsWep.com. [Viitattu 26.3.2015]. Saatavissa: http://www.tutorialsweb.com/rfid/index.htm

Corum, C. 2005. Understanding the different memory types used in contactless smart cards and RFID tokens. [verkkosivu]. AVISIAN Publishing. [Viitattu 28.3.2015]. Saatavissa: http://www.secureidnews.com/news-item/understanding-the-different-memory-types-used-in-contactless-smart-cards-and-rfid-tokens/

Franken, Z. 2008. PHYSICAL ACCESS CONTROL SYSTEMS. [Verkojulkaisu]. UBM Tech. [Viitattu 30.3.2015]. Saatavissa:

https://www.blackhat.com/presentations/bh-dc-08/Franken/Presentation/bh-dc-08-franken.pdf

EMVCo. 2011. EMV Integrated Circuit Card Specifications for Payment Systems; Book 3: Application Specification. [Verkkojulkaisu]. EMVCo LLC. [Viitattu 30.3.2015]. Saatavissa: http://www.emvco.com/download_agreement.aspx?id=654

Thompson, D. 2008. Lesson Title: RFID Modulation, Encoding, and Data Rates. [Verkkojulkaisu]. University of Arkansas, College of Engineering. [Viitattu: 30.3.2015]. Saatavissa: http://rfidsecurity.uark.edu/downloads/slides/mod04_lesson04_slides.pdf

EPCglobal. 2005. EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communication at 860 MHz – 960 MHz. [Verkkojulkaisu]. GS1 AISBL. [Viitattu 30.3.2015]. Saatavissa: http://www.gs1.org/sites/default/files/docs/epc/uhfc1g2_1_1_0-standard-20071017.pdf

Sherz, P. 2007. Practical Electronics for Inventors, Second Edition. McGraw-Hill.

MAINtag. 2014. MAINtag Introduces FLYchip64, the Highest-Performing RFID Memory Chip Meeting ATA Spec 2000 Standards. [verkkosivu]. PR Newswire Association LLC. [Viitattu 30.3.2015]. Saatavissa: http://www.prnewswire.com/news-releases/maintag-introduces-flychip64-the-highest-performing-rfid-memory-chip-meeting-ata-spec-2000-standards-245179911.html

EPCglobal. 2013. EPC Radio-Frequency Identity Protocols Generation-2 UHF RFID. [Verkkojulkaisu]. GS1 AISBL. [Viitattu 30.3.2015]. Saatavissa: http://www.gs1.org/sites/default/files/docs/epc/uhfc1g2_2_0_0_standard_20131101.pdf

HID Global. 2006. FlexKey Keytag. [Verkkojulkaisu]. Galaxy Control Systems. [Viitattu 30.3.2015]. Saatavissa: http://www.galaxysys.com/data/docs/1407954514_hid-understanding_card_data_formats-wp-en.pdf

NFC Forum. 2006. NFC Data Exchange Format (NDEF). [Verkkojulkaisu]. NFC Forum. [Viitattu 30.3.2015]. Saatavissa: http://members.nfc-forum.org/specs/spec_license/document_form/custom_layout?1427738926323 Vaatii kirjautumisen palveluun.

Suprina, D. 2005. Security Risks With RFID. [verkkosivu]. RFID Journal LLC. [Viitattu 1.4.2015]. Saatavissa: http://www.rfidjournal.com/articles/view?1564

IZT, Empa & BSI. 2004. Security Aspects and Prospective Applications of RFID Systems. [Verkkojulkaisu]. Bundesamt für Sicherheit in der Informationstechnik. [Viitattu 31.3.2015]. Saatavissa: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/RFID/RIKCHA_englisch_Layout_pdf.pdf;jsessionid=6E6A4D73F24D45713130FD7489255E24.2_cid359?__blob=publicationFile

Dayal, G. 2008. How they hacked it: The MiFare RFID crack explained. [verkkosivu]. Computerworld Inc. [Viitattu 31.3.2015]. Saatavissa: http://www.computerworld.com/article/2537817/security0/how-they-hacked-it--the-mifare-rfid-crack-explained.html

Biddle, S. 2012. The Simple, Brilliant Way to Stop RFID Robbers. [verkkosivu]. Gizmondo. [Viitattu 1.4.2015]. Saatavissa: http://gizmodo.com/5886355/the-simple-brilliant-way-to-stop-rfid-robbers

Bishop Fox. 2013. Tastic RFID Thief. [verkkosivu]. BISHOP FOX. [Viitattu 31.3.2015]. Saatavissa: http://www.bishopfox.com/resources/tools/rfid-hacking/attack-tools/

Gaudi, S. 2008. RFID hack could crack open 2 billion smart cards. [verkkosivu]. Computerworld Inc. [Viitattu 31.3.2015]. Saatavissa: http://www.computerworld.com/article/2537619/mobile-apps/rfid-hack-could-crack-open-2-billion-smart-cards.html

Brown, F. 2013. RFID Hacking: Live Free or RFID Hard. [Verkojulkaisu]. BISHOP FOX. [Viitattu 31.3.2015]. Saatavissa: http://www.bishopfox.com/download/837/

Paget, C. 2007. RFID for Beginners++. [Verkojulkaisu]. UBM Tech. [Viitattu 31.3.2015]. Saatavissa: https://www.blackhat.com/presentations/bh-usa-07/Paget/Presentation/bh-usa-07-paget.pdf

HS. 2014. Jo sadoillatuhansilla suomalaisilla on lähimaksukortti. [verkkosivu]. Helsingin Sanomat. [Julkaistu 26.12.2014]. [Viitattu 31.3.2015]. Saatavissa: http://www.hs.fi/talous/a1419560430271

Kalmi, R. 2013. Pankit tuputtavat uutta tekniikkaa – kuluttajia pelottaa. [verkkosivu]. Taloussanomat. [Julkaistu 5.6.2013]. [Viitattu 31.3.2015]. Saatavissa: http://www.taloussanomat.fi/raha/2013/06/05/pankit-tuputtavat-uutta-tekniikkaa-kuluttajia-pelottaa/20137977/139

OP. Ei päiväystä. Lähimaksu. [www-dokumentti]. Osuuspankki. [Viitattu 31.3.2015]. Saatavissa: https://www.op.fi/op/henkiloasiakkaat/kortit/kortin-kaytto/lahimaksu?cid=151670031&srcpl=3

Nordea. Ei päiväystä. Lähimaksaminen. [verkkosivu]. Nordea Pankki Suomi Oyj [Viitattu 31.3.2015] Saatavissa:

http://www.nordea.fi/Henkil%C3%B6asiakkaat/P%C3%A4ivitt%C3%A4iset+raha-asiat/Kortit/L%C3%A4himaksaminen/1607912.html?searchPhrase=l%u00e4hi&bb=0

Nixu. 2013. Etäluettavien maksukorttien turvallisuudesta. [verkkosivu]. Nixu Oyj. [Viitattu 31.3.2015] Saatavissa: http://www.nixu.com/fi/blogi/2013-05/et%C3%A4luettavien-maksukorttien-turvallisuudesta

Schwartz, J. 2006. Researchers See Privacy Pitfalls in No-Swipe Credit Cards. [verkkosivu]. The New York Times Company. [Julkaistu 23.10.2006]. [Viitattu 31.3.2015] Saatavissa: http://www.nytimes.com/2006/10/23/business/23card.html?sq=RFID%20identity%20theft&st=cse&scp=2&pagewanted=all&_r=0

Lee, E. 2012. NFC Hacking: The Easy Way. [Verkojulkaisu]. Korben.info. [Viitattu 31.3.2015]. Saatavissa: http://korben.info/wp-content/uploads/defcon/SpeakerPresentations/Lee/DEFCON-20-Lee-NFC-Hacking.pdf

Tait, D. 2014. NFC-Enabled Cellphone Shipments to Soar Fourfold in Next Five Years. [verkkosivu]. IHS In. [Viitattu 31.3.2015] Saatavissa: https://technology.ihs.com/490062/nfc-enabled-cellphone-shipments-to-soar-fourfold-in-next-five-years

Diakos, T.,Briffa, J.,Brown, T. & Wesemeyer, S. Eavesdropping near-field contactless payments: a quantitative analysis. [Verkkojulkaisu]. The Institution of Engineering and Technology. [Viitattu 1.4.2015]. Saatavissa: http://digital-library.theiet.org/docserver/fulltext/10.1049/joe.2013.0087/JOE.2013.0087.pdf?expires=1427888678&id=id&accname=guest&checksum=10C50DAA7ABEC30E532C0E93B1F81A60

Zetter, K. 2007. Open Sesame: Access Control Hack Unlocks Doors [verkkosivu]. Condé Nast. [Viitattu 31.3.2015]. Saatavissa: http://www.wired.com/2007/08/open-sesame-acc/