RADIOTAAJUINEN ETÄTUNNISTUS

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Syksy 2007
Tomi Salmi

Lahden ammattikorkeakoulu

Tietotekniikan koulutusohjelma

SALMI, TOMI: Radiotaajuinen etätunnistus

Tietoliikennetekniikan opinnäytetyö, 79 sivua

Syksy 2007

TIIVISTELMÄ

Tämä opinnäytetyö käsittelee radiotaajuuksilla toimivaa etätunnistusta. Radiotaajuustunnistus (RFID, Radio Frequency IDentification) mahdollistaa tiedon langattoman etäluvun ja -tallennuksen tunnisteiden eli tagien avulla. RFID on nopeasti yleistymässä oleva tekniikka, jolla on lukuisia sovellusmahdollisuuksia monilla eri aloilla.

RFID-järjestelmä koostuu pääasiassa lukijalaitteesta, tunnistettaviksi tai seurattaviksi tarkoitettuihin kohteisiin kiinnitetyistä tunnisteista sekä tietojärjestelmästä. Lukijalaite lähettää antenninsa välityksellä signaalin tunnisteelle, joka vastaa tähän toisella signaalilla. Signaalien välityksellä lukijalaitteen ja tunnisteiden välillä liikkuu energiaa ja järjestelmästä riippuvaa dataa. Tunnisteeseen voidaan tallentaa yksilöllisen sarjanumeron lisäksi tietoa esimerkiksi tuotteen valmistusprosessista tai tuotantoajankohdasta.

RFID-tekniikkaa voidaan käyttää muun muassa logistiikassa, vähittäiskaupassa, kulunvalvonnassa, joukkoliikenteessä, kirjastossa tai kotieläinten merkitsemisessä. RFID-tunnisteet ovat vähitellen korvaamassa viivakoodeja. Toisin kuin viivakoodit, tunnisteet toimivat ilman suoraa näköyhteyttä lukijaan ja pystyvät sisältämään huomattavasti enemmän tietoa. Lisäksi lukijat pystyvät käsittelemään monia tunnisteita samanaikaisesti.

Tunnistustekniikan haasteita ovat tällä hetkellä yhtenäisten kansainvälisten standardien luominen, kustannusten karsiminen sekä kuluttajan yksityisyydestä huolehtiminen. Lisäksi pohditaan, miten tekniikka pystyttäisiin tuomaan ihmisten arkeen mahdollisimman helppokäyttöisenä, luotettavana ja tietoturvallisena.

Avainsanat: RFID, radiotaajuustunnistus, tunniste, viivakoodi

Lahti University of Applied Sciences

Faculty of Technology

SALMI, TOMI: Radio Frequency Identification

Bachelor's Thesis in Telecommunications Technology, 79 pages

Autumn 2007

ABSTRACT

The aim of this thesis is to examine Radio Frequency IDentification (RFID). RFID is a rising identification technology that makes it possible to identify products wirelessly using radio waves. It has many possible applications in a wide range of areas.

An RFID system comprises three principal components. The first is the transponder, which is attached to the item that is to be tracked or identified. The second is the reader, which identifies the transponder, reads data from it, writes data to it and communicates with a data collection application. The data collection application enters the data into a database and provides access to the data.

RFID technology can be used for example in logistics, retail trade, access controlling, public transport or libraries. RFID transponders, called tags, are gradually replacing bar codes. Contrary to bar codes, tags are able to work without a visual connection to a reader and they can carry much more information. In addition, readers are able to handle many tags simultaneously.

The new identification technology also has its challenges. The biggest ones are creating common standards and cutting down the costs. To be accepted by the customers, RFID usage in customer relationship management has to meet certain requirements. The use of tags must be cheap, easy and reliable enough for customers, and it must not endanger their privacy.

Key words: RFID, radio frequency identification, transponder, tag, bar code

SISÄLLYS

TYÖSSÄ KÄYTETYT LYHENTEET

ASK	Amplitude-Shift Keying, modulaatiomenetelmä, jossa kantoaallon amplitudia muutetaan informaatiosignaalin mukaan
BPSK	Binary Phase-Shift Keying, modulaatiomenetelmä
CICC	Close-coupled Integrated Circuit Card, eli lyhyen kantaman kortti
EAN	European Article Number, eurooppalainen viivakoodistandardi
EAS	Electric Article Surveillance on RFID:n kaltainen, mutta huomattavasti yksinkertaisempi tekniikka
EEPROM	Electronically Erasable Programmable Read-Only Memory, puolijohdemuistityyppi
EIRP	Equivalent Isotropically Radiated Power, efektiivinen isotrooppinen säteilyteho
EPC	Electronic Product Code, sähköinen tuotekoodi
EPCIS	EPC Information Service, EPC-tuotetietoa sisältävä palvelin
FSK	Frequency-Shift Keying, modulaatiomenetelmä, jossa kantoaallon vaihetta muutetaan informaatiosignaalin mukaan
HF	High Frequencies, korkeat taajuudet; viittaa taajuusalueeseen 3–30 MHz
ICAO	International Civil Aviation Organization, kansainvälinen siviili-ilmailujärjestö

IEC	International Electrotechnical Commission, kansainvälinen elektroniikkaan erikoistunut standardointiorganisaatio
IFF	Identify Friend or Foe, brittien toisen maailmansodan tutkajärjestelmä, joka osasi erottaa omat lentokoneet vihollisen koneista
ISM	Industrial, Scientific, Medical, eli ISM-taajuusalueet ovat kaikkien vapaasti käytettävissä olevia taajuusalueita
ISO	International Organization for Standardization on kansainvälinen standardointiorganisaatio
LDS	Logical Data Structure, mikrosirun tietorakenne
LF	Low Frequencies, matalat taajuudet; viittaa taajuusalueeseen 30–300 kHz
MRTD	Machine Readable Travel Document, koneluettava matkustusasiakirja
NFC	Near Field Communication, RFID:hen pohjautuva radiotaajuinen etätunnistustekniikka
NRZ	Non-Return to Zero, koodausmenetelmä
NRZI	Non-Return to Zero Inverted, NRZ:n kehittyneempi malli
ONS	Object Name Service, EPC-verkon objektien nimipalvelin
PICC	Proximity Integrated Circuit Card, lähilukukortti
PCD	Proximity Coupling Device, lähilukukortin lukijalaite
RFID	Radio Frequency Identication on radiotaajuustunnistamista

PPM	Pulse Position Modulation, eräs modulointimenetelmä
PSK	Phase-Shift Keying, modulaatiomenetelmä, jossa kantoaallon vaihetta muutetaan informaatiosignaalin mukaan
SRD	Short-Range Devices, lyhyen kantaman langattomat sovellukset
UHF	Ultra High Frequency, taajuusalue, viittaa taajuuksiin 300 MHz – 3 GHz
UWB	Ultra Wideband, laajan taajuuskaistan radioteknologia
UPC	Universal Product Code, kansainvälinen tuotekoodi
VICC	Vicinity Integrated Circuit Card, etälukukortti
VDC	Vicinity Coupling Device, etälukukorttien lukulaite
VHF	Very High Frequency, taajuusalue, viittaa taajuuksiin 30–300 MHz
WLAN	Wireless Local Area Network, standardin IEEE 802.11 mukainen langaton lähiverkko

1 JOHDANTO

RFID (Radio Frequency Identification) on yleisnimitys radiotaajuuksilla toimivalle etätunnistusteknologialle. RFID-tekniikka on tällä hetkellä eräs tietotekniikan nopeimmin kehittyvistä sovellusalueista.

Tunnistettavaan kohteeseen, kuten esineeseen, ihmiseen tai eläimeen kiinnitetään tarkoitukseen suunniteltu tunniste, eli tagi. Tunniste sisältää tietoa, jonka perusteella se voidaan erottaa muista tunnisteista; tällaisia tietoja ovat muun muassa tuotteen sarjanumero, valmistuspäivä ja reitti tehtaalta kaupan hyllylle. Kun tunnisteen sisältämää tietoa halutaan lukea, lukijalaite lähettää sille signaalin. Tunniste vastaanottaa lähetteen, tulkitsee sen ja välittää lukijalaitteelle sen kaipaamat tiedot. Lukijalaite vastaanottaa ne ja yhdessä lukijaan liitetyn tietojärjestelmän kanssa tunnistaa, mistä tagista on kyse. Jatkotoimenpiteet riippuvat järjestelmästä.

RFID on yleistymässä nopeasti, koska yritykset ovat aina kiinnostuneita keinoista, joiden avulla voidaan alentaa kustannuksia. RFID voi tehostaa lukuisia prosesseja esimerkiksi logistiikassa automatisoimalla lähetys- ja vastaanottotoimintoja sekä mahdollistamalla tarkan kuljetusten seurannan. RFID on jo jossain määrin korvannut viivakoodeja. Suurempi mullistus on yhä edessäpäin odottamassa uuden tekniikan kustannusten putoamista.

Opinnäytetyön tavoitteena on tutkia RFID-tekniikkaa, sen standardeja ja toteutusta sekä esitellä lyhyesti tekniikan toiminnan taustalla olevat fysikaaliset perusteet. Tarkoituksena on käsitellä myös tekniikan haasteita ja ongelmakohtia, kuten suurten tietomäärien yhtäaikainen käsittely sekä tietoturvaan ja kuluttajien yksityisyyteen liittyviä tekijöitä. Lisäksi perehdytään muutamiin RFID:n yleisimpiin käyttökohteisiin ja mietitään tekniikan tulevaisuutta.

2 AUTOMAATTINEN TUNNISTAMINEN

2.1 Radiotaajuustunnistuksen historia

Langatonta viestintää harrastettiin jo kauan ennen sähköisen langattoman tiedonsiirron keksimistä. Tunnettuja esimerkkejä ovat intiaanien käyttämät savumerkit. Sähköisen langattoman viestinnän juuret ulottuvat 1800-luvun alkupuolelle, jolloin Michael Faraday (1791–1867) keksi laitteen, joka muutti sähkövirran liikkeeksi. Tämä tapahtui vuonna 1821 ja kymmenen vuotta myöhemmin hän keksi magneettisen induktion pitkän ja johdonmukaisen kokeilun tuloksena. Vuonna 1845 Faraday esitteli sähköiset ja magneettiset voimat kenttinä. Näitä kenttiä hän nimitti voimaviivoiksi (engl. lines of force). (Granlund 2001, 4.)

James Clerk Maxwell (1831–1879) puki Faradayn ajatukset matemaattiseen muotoon, ja nykyään Maxwellin yhtälöt ovat yksi merkittävä kulmakivi sähkömagnetismin teoriassa. Sähkömagneettisen säteilyn havainnollisti ensimmäisenä saksalainen fyysikko Heinrich Hertz (1857–1894) vuonna 1888 rakentamalla radioaaltoja tuottaneen laitteen. Värähtelyn mittayksikkö Hz (hertsi) on nimetty Hertzin mukaan. Hertzin kuoltua hänen työtään jatkettiin, ja vuonna 1895 venäläinen Alexander Popov keksi, että myös salama tuottaa sähkömagneettista säteilyä. Hän myös tiettävästi ensimmäisenä onnistui muodostamaan radioyhteyden kahden pisteen välille, vaikka kunniaa tästä on annettu myös italialaiselle Guglielmo Marconille. (Granlund 2001, 5; Korpinen 2005.)

Marconi (1874–1937) ryhtyi vuonna 1895 tutkimaan radioaaltoja ja pian hän onnistui lähettämään viestin langattomasti muutaman kilometrin päässä olleelle vastaanottimelle. Seuraavana vuonna hänelle myönnettiin ensimmäinen sähköistä lennätintä koskeva patentti. 1800- ja 1900-lukujen vaihteessa Marconi kehitti ja patentoi lukuisia keksintöjä. Vuonna 1931 hän ryhtyi tutkimaan mikroaaltoja ja rakensi seuraavana vuonna ensimmäisen mikroaaltolinkin. Vuonna 1935 Marconi esitteli toimivan tutkan. (Granlund 2001, 5–6.)

RFID on terminä uusi, vaikka radiotaajuustunnistaminen on ollut teknisesti mahdollista jo vuosikymmeniä, ja sitä on käytetty pitkään muun muassa kulunvalvonnassa ja tietulleissa. Tekniikan käyttö on yleistynyt vasta aivan viime vuosina, ja varsinaiset huippuvuodet ovat yhä edessä. RFID-tekniikan juuret ulottuvat tutkan keksimiseen, eli vuoteen 1935 saakka. Tutkan toiminta perustuu havaittavista kohteista heijastuvaan säteilyyn, ja toisessa maailmansodassa tutkia käytettiin muun muassa lentokoneiden ja laivojen havaitsemiseen. Tekniikan rajoittuneisuuden vuoksi ensimmäiset tutkat eivät kuitenkaan osanneet tehdä eroa omien ja vihollisten välillä. Vuonna 1939 brittiläiset keksivät lisätä omiin lentokoneisiinsa lähettimen, joka osasi vastata erityisellä koodatulla tunnistussignaalilla heidän oman tutkansa lähettämään signaaliin. Järjestelmästä tuli maailman ensimmäinen RFID-järjestelmä, ja sitä kutsuttiin nimellä Identify Friend or Foe (IFF). (Goebel 2007.)

Ensimmäinen nykyaikaista RFID-tekniikkaa muistuttava patentti myönnettiin vuonna 1973 Mario Cardullolle. Patentti perustui passiiviseen (ei omaa virtalähdettä) tunnisteeseen, jossa oli myös pieni muistipiiri. Ensimmäinen patentti, jossa mainittiin lyhenne RFID, hyväksyttiin vuonna 1983 Charles Waltonille. (RFID Journal 2007.)

Ensimmäiset kaupalliset RFID-sovellukset nähtiin 1980-luvulla tietulleissa. Samaan aikaan RFID:n parissa työskentelevien ihmisten, yritysten ja tutkimuslaitosten määrä kasvoi huomattavasti. USA:ssa päähuomio oli kuljetussovelluksissa ja henkilöstön kulunvalvonnassa, kun taas Euroopassa keskityttiin kotieläinten lyhyen kantaman langattomaan tunnistamiseen ja teollisiin sovelluksiin. 80-luvulla otettiin käyttöön myös ensimmäiset hiihtokeskusten hissilippusovellukset. 90-luvulla tietullit jatkoivat kehittymistään, ja käyttöön otettiin järjestelmä, joka pystyi toimimaan moottoritienopeuksilla. (Kärkkäinen 2006.)

2000-luvun alussa kiinnostus etätunnistustekniikkaan kasvoi jyrkästi ja siitä ryhdyttiin odottamaan viivakoodien korvaajaa. Myös uusia sovellusalueita keksittiin jatkuvasti, kuten autojen varkaudenestojärjestelmät, maksutoimintojen hoitaminen huoltoasemilla sekä kirjastosovellukset osoittavat. Lisävauhtia ja

-julkisuutta RFID-tekniikka on saanut sen tunnetuilta käyttäjiltä, kuten Wal-Mart-kauppaketjulta ja Yhdysvaltain puolustusministeriöltä. Logistiikassa ja vähittäismyynnissä RFID on vähitellen korvaamassa viivakoodia. (Ojanperä 2004.)

2.2 Viivakoodi

RFID nähdään monilta osin viivakooditekniikan täydentäjänä ja pidemmällä aikavälillä myös korvaajana. RFID-tekniikka ei voi suoraan korvata laajasti käytössä olevaa perinteistä viivakoodia, koska teollisuus on niin vahvasti kiinni vanhassa järjestelmässä. RFID on kuitenkin tulossa käyttöön asteittain, koska sen edut verrattuna viivakoodiin ovat ilmeiset.

Kaupoissa on jo pitkään käytetty viivakoodeja, joiden avulla tuotteet pystytään tunnistamaan koneellisesti. Ennen viivakoodien käyttöönottoa jokaisen tuotteen hinta naputeltiin kauppojen kassoilla koneeseen käsin. Monissa tuotteissa oli hintalaput, sillä muutoin kassanhoitajan piti muistaa hinta ulkoa tai tarkistaa hinnastosta. Koneen antamasta kassakuitista näki lopuksi loppusumman ja listan yksittäisiä hintoja ilman tietoa siitä, mihin tuotteisiin ne liittyivät. Ensimmäiset viivakoodikokeilut tehtiin Yhdysvalloissa 1960-luvun alussa, kun rautatieyhtiöt merkitsivät viivakoodeilla tavaravaunujaan. Koodien avulla vaunujen liikkeiden seuranta pitkin valtavaa mannerta oli helpompaa kuin kynällä ja paperilla. (Majander 2004.)

Vuonna 1967 viivakoodia kokeiltiin ensimmäistä kertaa kaupan tuotteiden merkintään Cincinnatissa Yhdysvalloissa. Koodi muodostui ympyränmuotoisista viivoista. Kullakin viivakoodeja käyttäneellä liikkeellä oli aluksi oma muiden kanssa epäyhteensopiva koodistonsa, kunnes vuonna 1970 ryhdyttiin kehittämään yhtenäistä merkintätapaa. Ensimmäinen standardoitu nykymuotoinen tuotekohtainen viivakoodi syntyi vuonna 1974, ja se kiinnitettiin purukumipakettiin. (Majander 2004; Adams 2007.)

Eri käyttötarkoituksia varten on kehitetty erilaisia viivakoodityyppejä, jotka eroavat toisistaan muun muassa merkistöltään, ulkonäöltään ja pituudeltaan. Kaikissa on silti sama perusperiaate, koodissa vuorottelevat valoa heijastavat ja heijastamattomat kohdat. Yleisimmin käytetty viivakoodityppi on yksiulotteinen viivajono (KUVIO 1.), joka luetaan yhdellä pyyhkäisyllä päästä toiseen. Kuvion koodaamaa tietomäärää voidaan kasvattaa vain viivajonoa pidentämällä. (Majander 2004.)

KUVIO 1. Perinteinen yksiulotteinen viivakoodi

KUVIO 2. Kaksiulotteinen viivakoodi (AINO 2006.)

Kaksiulotteiset viivakoodit (KUVIO 2.) ovat yksiulotteisia kehittyneempiä. Niissä tieto koodataan useammalle riville, jolloin viivastoja on useita päällekkäin. Tuloksena saadaan esimerkiksi neliön muotoinen mustavalkoinen kuvio. Kaksiulotteisten viivakoodien etuna on mahdollisuus sijoittaa pienelle alueelle huomattavasti entistä suurempi määrä dataa. Toisaalta pienikin tahra tekee siitä helposti lukukelvottoman, kun taas selkeämpi yksiulotteinen viivakoodi säilyy luettavana, vaikka osa siitä suttaantuisi. Kaksiulotteisia viivakoodeja ei voi lukea perinteisillä lukulaitteilla, vaan ne vaativat erityisesti niitä varten suunnitellut lukulaitteet. (Majander 2004.)

Standardista riippuen viivakoodilla voidaan esittää joko pelkkiä numeroita tai vaihtoehtoisesti sekä numeroita että kirjaimia. Yksinkertaisimmissa viivakoodityypeissä numerot on koodattu vaihtelemalla viivojen leveyttä. Yleensä sekä viivojen että välien leveydet vaihtelevat. Viivakoodeissa käytetään tavallisesti neljää eri viivan tai välin leveyttä siten, että ohuimman viivan leveys on koodin

perusyksikkö ja muut leveydet sen kerrannaisia. Koska yksittäisellä viivalla ja välillä voi olla vain neljä arvoa, muodostuu kukin numero tai kirjain useammasta viivasta ja välistä. Varsinaisen sisällön eli hyötydatan lisäksi kukin viivakoodi sisältää myös vaihtelevan määrän ohjaustietoa, jonka avulla lukulaite pystyy päättelemään perusviivan leveyden ja koodin lukusuunnan. (Majander 2004.)

Suomen ja muun Euroopan vähittäiskaupassa viivakoodeissa käytetään EAN-13-koodia (European Article Number). Nimensä mukaisesti se ilmaisee 13 numeromerkkiä, joista kaksi tai kolme ensimmäistä on varattu maakoodille. Suomen maakoodi on 64. Seuraavaksi EAN-koodi sisältää yritysnumeron sekä tuotteen numeron. Yritys- eli valmistajanumerot jakaa kussakin maassa viivakoodeista vastaava viranomainen, joka Suomessa on GS1 Finland Oy (entinen EAN Finland Oy). Tuotenumerot kukin yritys määrittelee itse. Yritys- ja tuotenumeroiden pituudet vaihtelevat. Jos yrityksen tuotevalikoima on laaja, sille annetaan lyhyt yritysnumero, jolloin tuotenumeroille jää enemmän tilaa. Vastaavasti suppeamman tuotevalikoiman valmistaja saa pidemmän yritysnumeron. Viimeisenä EAN-koodissa on tarkistusluku, jonka perusteella lukulaite varmistaa, että koodi on luettu oikein. (Majander 2004.)

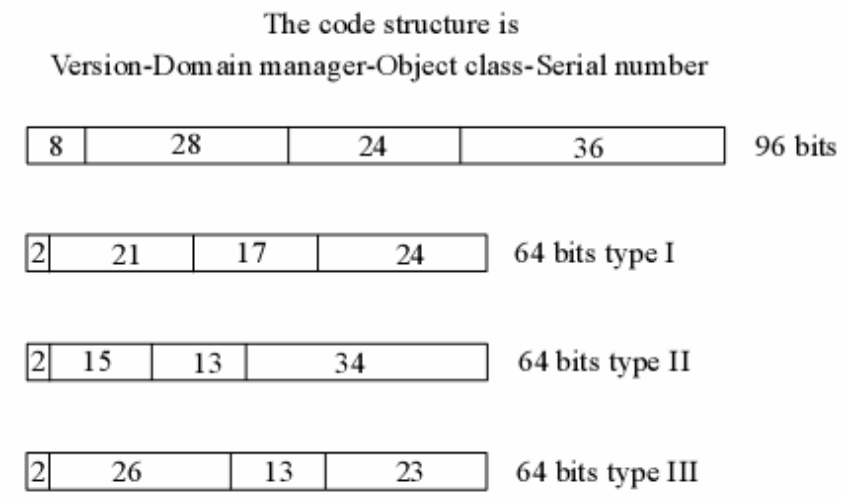
Viivakoodi ei sisällä tietoa tuotteen hinnasta. Viivakoodi pelkästään kertoo kassakoneelle tai muulle laitteelle mistä tuotteesta on kyse, eli sen avulla tunnistetaan tuote. Tuotenumero välitetään tietokantaan, josta tuotenumeron perusteella poimitaan hinta. Kun hinnat ovat keskitetysti yhdessä paikassa, esimerkiksi hintoja muutettaessa muutokset tarvitsee tehdä vain hintatietokantaan, ei jokaiseen tuotteeseen yksitellen. (Majander 2004.)

2.3 Sähköinen tuotekoodi

RFID-tunnisteet sisältävät usein yksilöivän sähköisen tuotekoodin (EPC, Electronic Product Code), joka on huomattavasti pidempi kuin viivakoodeissa yleisesti käytetty EAN-viivakoodi tai kansainvälinen tuotekoodi (UPC, Universal Product Code). EPC on 64-, 96- tai 256-bittinen koodi, joka on jaettu erilaista

tietoa sisältäviin numerosarjoihin. Tällaista tietoa ovat muun muassa tuotteen valmistaja ja tuotetyyppi. Koodin pituuden ansiosta jokaiselle tuotteelle voidaan antaa oma yksilöivä koodinsa sen sijaan, että käytettäisiin tuoteryhmittäin jaettuja sarjanumeroita. Yksilöinnin ansiosta yksittäisillä koodeilla varustettuja tuotteita on mahdollista seurata niiden koko elinkaaren ajan. EPC:n standardointia koordinoi maailmanlaajuisesti EPCglobal Inc. (EPCglobal 2006.)

EPC-koodin kehys koostuu otsikosta ja varsinaisesta tuotetunnuksesta. Kehyksen otsikkokenttä määrittää koodin version, pituuden, rakenteen, tyypin ja EPC-sukupolven. Tuotetunnusosuus on jaettu kolmeen osaan, jotka merkitsevät tuotteen valmistajaa (domain manager), tuoteryhmää (object class) ja tuoteyksilöä (serial number). Osien pituudet vaihtelevat versioittain (KUVIO 3.). (EPCglobal 2006.)



KUVIO 3. Esimerkkejä muutamista EPC-koodeista (EPCglobal 2006.)

2.4 RFID:n ja viivakoodin vertailua

Radiotaajuustunnistus ja viivakoodi edustavat eri teknologiaa, vaikka niillä onkin osittain yhteneväiset käyttötavat (TAULUKKO 1.). Suurin ero tekniikoiden välillä on, että viivakoodi edellyttää esteetöntä näköyhteyttä lukijan ja vii-

vakoodin välillä. Tästä syystä käyttäjän on suunnattava viivakoodi lukijaa kohti. RFID-tunniste sen sijaan voidaan lukea ilman näköyhteyttä, kunhan se on lukijan lukuetäisyyden sisällä eli lukualueella. Viivakoodin edellyttämä näköyhteys lukijaan vaatii samalla, että viivakoodi kiinnitetään tuotepakkauksen ulkopintaan, jossa viivakoodi altistuu kulutukselle, lialle sekä pölylle ja voi irrota tai repeytyä lukukelvottomaksi. RFID-tunniste sen sijaan voidaan pääsääntöisesti sijoittaa tuotepakkauksen sisään, jossa se on turvassa useimmilta ympäristön mahdollisilta häiriötekijöiltä. RFID-tunniste helpottaa ja nopeuttaa tuotteiden käsittelyä esimerkiksi varastoissa ja kassoilla, sillä tuotteita ei tarvitse viivakoodin tapaan käsitellä yksitellen, vaan RFID-lukijat pystyvät käsittelemään sekunnissa satoja tunnisteita ilman manuaalisesti tehtävää tarkkaa kohdistusta. (AINO 2006.)

Viivakoodin sisältämä informaatio on staattista eli muuttumatonta, eli siihen talletettua tietoa ei voi jälkikäteen muuttaa. RFID-tagit sen sijaan voivat olla uudelleenkirjoitettavia, jolloin niiden sisältämä tieto on muokattavissa tunnisteen tyypistä riippuen. (Christensen 2007.)

Tekniikoiden paremmuus riippuu aina käyttöympäristöstä. Usein varsinkin siirtymävaiheessa mikrosirun sisältämässä RFID-tarrassa on myös viivakoodi, sillä viivakoodista ei yleensä voida luopua heti radiotaajuustunnistuksen käyttöönoton jälkeen. Koodi tai selväkielinen teksti toimii myös varajärjestelmänä siltä varalta, että tunnistetta ei saada luettua tarkoituksenmukaisilla lukulaitteilla. Perinteinen viivakoodi pystyy tunnistamaan tuotetyypin tai -nimikkeen yleisellä tasolla, mutta rajallisen tietomääränsä vuoksi se ei kykene yksilöimään yksittäistä tuoteyksilöä. Ruokakaupassa omena on viivakoodille omena, mutta RFID:llä tietomäärää pystytään kasvattamaan, jolloin kustakin tuotteesta voidaan tallentaa esimerkiksi viimeinen myyntipäivä ja alkuperämaa. Tagien avulla voidaan myös seurata, miten juuri jokin tietty tuote on kulkenut jakeluketjussa tai esimerkiksi kuinka tuore se on. Tunnisteesta riippuen siihen voidaan tallentaa tietoa myös jälkikäteen, jolloin informaatiota pystytään päivittämään lennossa, mikä on viivakoodeilla mahdotonta. (Christensen 2007.)

Tiivistetysti voidaan sanoa, että RFID-tekniikka häviää viivakoodeille vain kustannuksissa ja rajoittuneessa toimivuudessa joidenkin aineiden lähettyvillä.

TAULUKKO 1. Viivakoodin ja RFID-tekniikan vertailua (AINO 2006; Kalliokoski 2007.)

Ominaisuus	**Viivakoodi**	**RFID**
Näköyhteys	Vaaditaan.	Ei vaadita.
Moniluku	Ei mahdollista.	Mahdollista.
Lukuetäisyys	Alle 1 m	n. 0,5 m (passiivinen, LF-alue) – n. 100 m (aktiivinen).
Valaistus	Vaaditaan.	Ei vaadita.
Tallennuskapasiteetti	Yleensä n. 50 merkkiä.	64 – 1024 bit (passiivinen), 32 kbit (aktiivinen)
Tiedon muokkaus	Ei mahdollista. Staattinen sisältö.	Riippuen tunnisteesta. Usein dynaaminen (luku/kirjoitus).
Standardisointi	GS1	EPCglobal, ISO
Kiinnityspinta / tietyn materiaalin läheisyys	Lukusignaali ei läpäise nestettä / metallia.	Riippuen järjestelmästä, esim. metalli ja nesteet voivat häiritä lukua.
Herkkyys lialle	Häiritsee / estää luvun.	Ei haittaa.
Tunnisteen hinta	Lähes ilmainen.	Vaihtelu suurta, passiivinen n. 0,1 – 0,5 €, aktiivinen n. 20 €
Lukijan hinta	100 – 300 € (pistooli)	100 – 500 € (kannettava) 1000 – 5 000 € (kiinteä)
Kopioitavuus	Helppo väärentää.	Vaikea väärentää.
Tunnistaminen	Vaatii manuaalista työtä.	Automaattinen.
Varajärjestelmä	Selväkielinen teksti.	Viivakoodi / selväkielinen teksti.

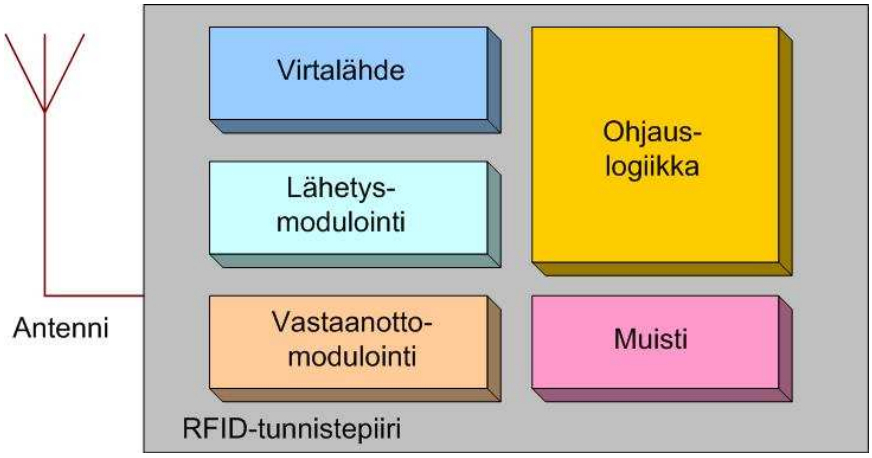
3 RFID-JÄRJESTELMÄ

3.1 Tunnisteet

3.1.1 Tunnisteen rakenne

RFID-järjestelmä koostuu kolmesta pääkomponentista: tunnisteista, lukijalaitteesta sekä tietojärjestelmästä. RFID-tunniste on pieni laite, joka kiinnitetään seurattavaan tai tunnistettavaksi tarkoitettuun kohteeseen. Tunniste (KUVIO 4.) sisältää tietoa esineestä tai tuotteesta johon se on kiinnitetty ja sen sisältö voidaan lukea langattomasti RFID-lukijalaitteilla. Tunnisteita kutsutaan myös nimillä tagi, saattomuisti tai älytarra. Merkittävästä tuotteesta riippuen tunniste voidaan sisällyttää siihen jo valmistusvaiheessa tai esimerkiksi liimata jälkikäteen tarralla.

Tunnisteita on käytössä lukuisia erilaisia (KUVIO 5.), ja ne ovat usein juuri tiettyyn käyttötarkoitukseen suunniteltuja. Tunnisteet ovat yleensä alle tulitukkirasian kokoisia, ja ne sisältävät langattomaan tiedonsiirtoon käytettävän antennin sekä tietosirun, johon tieto on tallennettu. Tagien ominaisuudet vaihtelevat muun muassa energianlähteen, käytetyn taajuuden, fyysisen koon sekä tallennuskapasiteetin mukaan. Kun etsitään parasta tunnistetyyppiä tiettyyn käyttökohteeseen, täytyy pohdinnoissa ottaa huomioon kaikki eri ominaisuuksien tuomat mahdollisuudet ja rajoitukset. (VTT 2004.)



KUVIO 4. RFID-tunnisteen rakenne

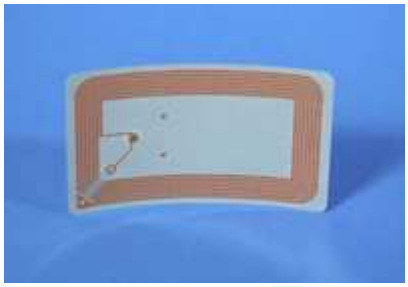
Tunnisteen ulkoisesti näkyvin osa on antenni, jota käytetään tiedon vastaanottamiseen ja lähettämiseen langattomasti lukijalaitteelle. Yleisesti voidaan sanoa, että mitä suurempi antenni on, sitä paremmat lukuetäisyydet voidaan saavuttaa. Lukuetäisyydet riippuvat kuitenkin aina myös käytetystä taajuudesta sekä tunnisteen asennosta ja esimerkiksi kiinnitystavasta. Jos tagin käyttökohde tunnetaan tarkasti jo suunnitteluvaiheessa, pystytään sen koko ja muut yksityiskohdat optimoimaan juuri tulevaa käyttötarkoitusta silmälläpitäen. Samalla säästetään valmistusmateriaaleja, mikä näkyy aina myös loppuhinnassa. (ToP Tunniste 2006.)

KUVIO 5. Erilaisia RFID-tunnisteita (Tamtron Solutions Oy 2007.)

Tagit eivät välttämättä ole pelkästään mukana kulkevia langattomasti luettavia saattomuisteja, vaan niiden yhteyteen voidaan liittää myös muunlaisia toimintoja. Esimerkiksi lämpöanturiin liitetty tagi voi toimia muistia sisältävänä lämpömittarina, johon anturin mittaamat tiedot tallentuvat tietyin väliajoin. Kun paikalle tuodaan kannettava lukijalaite, tiedot siirtyvät tagista lukijalaitteen muistiin, josta ne puolestaan voidaan siirtää suurempaan tietokantaan myöhempää ja mistä tahansa tehtävää tarkastelua varten. (VTT 2004.)

RFID-tunnisteiden tavallisin rakennetyyppi on inletti. Muita tyyppejä ovat esimerkiksi älytarrat, kontaktittomat älykortit, ulkotilojen tarrat ja kovat tunnisteet. Inletti (KUVIO 6.) on yksinkertaisin tunnistetyyppi ja se toimitetaan

yleensä kelana. Inletin näkyvin osa on kierretty antenni, jonka koko määrää koko tunnisteen koon. Inletin pinta on yleensä synteettistä muovia ja sen kääntöpuolella on tavallisesti liimapinta, jolla se voidaan kiinnittää kohteeseen. Inletit soveltuvat parhaiten tuotteisiin, joissa se voidaan kiinnittää tuotteen sisään tai pinnan alle. (ToP Tunniste 2006.)



KUVIO 6. Inletti (Top Tunniste 2006.)

KUVIO 7. Nappimainen Kova tagi hankaliin olosuhteisiin (ToP Tunniste 2006.)

Älytarrojen pintamateriaali vaihtelee, mutta on yleensä synteettistä muovia vaihtelevalla painatuksella. Tarran kääntöpuolalla on liimapinta ja ne toimitetaan keloina. Älytarrassa olevan tunnisteen inlettikoko tulee olla pienempi kuin pintamateriaalin. Tunnisteita löytyy erityyppisiä muun muassa mikropiirin valmistajan, kommunikointiprotokollan tai taajuuden mukaan. (ToP Tunniste 2006.)

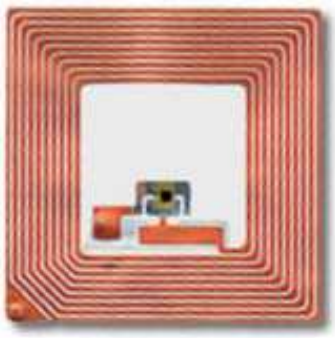
RFID-älykortit ovat luottokortin kokoisia sekä näköisiä, ja niitä käytetään yleensä henkilötunnistuksessa ja muun muassa pääkaupunkiseudun joukkoliikenteessä. Pintamateriaali on synteettistä muovia, ja niiden pintaan voidaan painattaa erilaisia tekstejä ja kuvia, kuten logoja. Korteista kerrotaan lisää luvussa 5 Kontaktittomat älykortit. (ToP Tunniste 2006.)

Niin sanottuja kovia tageja (KUVIO 7.) käytetään vaikeissa olosuhteissa, joissa tunniste voi joutua kemikaalien tai muunlaisen kulutuksen kohteeksi. Kestävän

pintamateriaalin vuoksi ne sopivat hyvin ulkoilmaan ja toimivat myös metallin päällä. Kovien tagien ulkonäkö vaihtelee suuresti, ja usein ne valmistetaan tiedetyn käyttökohteen mukaan kohteen ulkoasuun sopivaksi. Kiinnitys tapahtuu liimalla tai esimerkiksi mekaanisesti ruuvin avulla. (ToP Tunniste 2006.)

3.1.2 Passiivinen tai aktiivinen tunniste

Tunnisteet voivat olla energianlähteensä perusteella joko passiivisia, semi- eli puolipassiivisia tai aktiivisia. Passiivisissa tunnisteissa (KUVIO 8.) ei ole erillistä virtalähdettä, vaan ne saavat tarvitsemansa energian lukijalaitteen lukukentästä. Lukijalaite kehittää magneettikentän tai sähkömagneettista säteilyä, jonka synnyttämä sähkökenttä tuottaa passiivisen tunnisteen tarvitseman energian. Syntyvä sähkövirta siirtyy tunnisteessa antennia pitkin pienelle elektroniselle piirille, josta luetaan edelleen takaisin lukijalle lähetettävät tiedot. (VTT 2004.)



KUVIO 8. Tyypillinen passiivinen RFID-tunniste (Estelle Networks 2006.)

Koska passiivisissa tunnisteissa ei ole omaa virtalähdettä, ne ovat täysin riippuvaisia lukijan luomasta lukukentästä. Kaikki viestintä on mahdollista vain, kun tunniste on lukijan kentässä. Samasta syystä passiiviset tunnisteet eivät toimi kovin kaukana lukijasta, koska pelkkä lukijalaitteen kentästä tunnisteelle välittyvä energia ei riitä pitkillä matkoilla riittävän tehokkaan lähetyssignaalin luomiseen. Haittapuolien lisäksi rajoittuneella käyttöetäisyydellä on myös omat etunsa, sillä tagin tahaton käyttö estyy tehokkaasti, tietoturva paranee ja yksityisyyden loukkaamisen mahdollisuudet vähenevät. Koska omaa virtalähdettä ei ole, passiiviset tunnisteet ovat aktiivisia tunnisteita pienempiä, halvempia ja niillä on periaatteessa rajaton käyttöikä. Paristottoman passiivitunnisteen etuna on myös ympäristöystävällisyys, ja se on vaaraton terveydelle. (VTT 2004; AINO 2006.)

Semipassiivisissa tunnisteissa on oma virtalähde, mutta sitä käytetään vain tietojen lähettämiseen lukijalle sen jälkeen, kun on ensin vastaanotettu lukijalta tuleva herätesignaali. Muuten semipassiivinen tunniste toimii kuten passiivinen tunniste. Oman virtalähteen ansiosta semipassiivisten tunnisteiden lukuetäisyys on passiivisia tunnisteita pidempi. Tyypillinen semipassiivisen tunnisteen käyttökohde on tietullien keräämiseen tarkoitettu järjestelmä. Kun auto saapuu tietullilukijan lukualueelle, lukija lähettää tunnisteelle herätesignaalin, jonka vastaanotettuaan tuulilasiin kiinnitetty semipassiivinen tunniste lähettää oman virtalähteensä voimalla tietonsa lukijalle. Näin lukija ja tietullien kerääjä saavat tietoonsa tunnisteeseen tallennetut tiedot, ja maksu osataan periä oikealta tienkäyttäjältä. Tagin oman virtalähteen ansiosta tietulli voidaan periä, vaikka auto liikkuu ja etäisyys lukijalaitteeseen on useita metrejä. (VTT 2004.)

Aktiivisissa tunnisteissa on oma sisäinen virtalähteensä, käytännössä paristo tai akku, minkä ansiosta niiden lukuetäisyys voi olla jopa kymmeniä metrejä. Kirjoitusetäisyydet ovat yleensä lukuetäisyyksiä lyhyempiä. Lisäksi tunnisteessa itsessään olevaa virtalähdettä voidaan käyttää tunnisteen oman laskennan virtalähteenä, jolloin esimerkiksi kirjoitusoperaatioiden suorittaminen on mahdollista myös ilman lukijalaitteen läsnäoloa. Tästä ominaisuudesta on hyötyä erityisesti, kun tunnistetta käytetään yhdessä erillisen anturin kanssa esimerkiksi lämpötilan mittauksessa. Tällöin anturin mittaamat lämpöarvot voidaan tallettaa tietyin väliajoin tunnisteen muistiin ja kun lukijalaite saapuu lukuetäisyydelle, tiedot voidaan siirtää eteenpäin erilliseen tietokantaan. (VTT 2004.)

Virtalähteen aiheuttamasta koon kasvusta johtuen aktiivisten tagien sijoittaminen on hieman hankalampaa ja siten niiden tyypilliset käyttökohteetkin ovat erilaisia kuin passiivisilla tunnisteilla. Useimmissa aktiivitunnisteissa virtalähde on kiinteästi osa tunnistinta, joten sen vaihtaminen on hyvin vaikeaa tai mahdotonta. Samalla käyttöikä on rajattu, ja paristo voi rajoittaa myös käytettävää lämpötila-aluetta. (AINO 2006.)

3.1.3 Muistit

Tunnisteiden tallennuskapasiteetin määrä vaihtelee muutamista kymmenistä biteistä muutamaan kilotavuun. Kaikkein yksinkertaisimpiin ja halvimpiin tunnisteisiin on tallennettu vain sen yksikäsitteinen, eli uniikki tunnistenumero, minkä lisäksi ne ovat vain kerran kirjoitettavia. Tämä tarkoittaa, että tieto on tallennettu tunnistimeen heti tehtaalla eikä muistin sisältöä voi jälkikäteen muuttaa, vaan tietoa voidaan pelkästään lukea. (VTT 2004.)

Tunnisteet voidaan jakaa muistin toimivuuden perusteella kolmeen tyhmään:

- RO = Read Only. Tunnisteen muistia voidaan vain lukea, tallennusmahdollisuutta ei ole.
- RW = Read / Write. Luku- ja kirjoitusmahdollisuus, eli tunniste on niin sanotusti uudelleenkirjoitettava.
- WORM = Write Once, Read Many. Muisti, johon voidaan tallentaa vain kerran, mutta jonka sisältö voidaan lukea monta kertaa.

(AINO 2006.)

Jos passiivisissa tunnisteissa halutaan käyttää tallennusmahdollisuutta, tällöin käytetään yleensä EEPROM-tyyppisiä (Electronically Erasable Programmable Read-Only Memory) muisteja. EEPROM on haihtumaton puolijohdemuisti, joka ei tarvitse käyttöjännitettä säilyttääkseen siihen tallennettua dataa.

3.2 Lukijalaitteet

Lukijalaite on tunnisteen ohella RFID-järjestelmän toinen oleellinen osatekijä. Sillä on lukuisia eri tehtäviä, kuten käyttöenergian siirtäminen passiiviselle tunnisteelle, tunnisteen identifiointi, sen lukeminen ja siihen kirjoittaminen sekä tietojen kuljetus tunnisteen ja tietojärjestelmän välillä. Lukijan on toimittava samalla taajuudella kuin sillä luettava tunniste, minkä lisäksi sen on oltava yhteensopiva myös muilta osin. Lukijaa ohjaava logiikka voi olla ohjelmoituna suoraan laitteeseen, tai se voi tulla ulkoisesta järjestelmästä. (VTT 2004.)

Kun tunniste saapuu lukijalaitteen lukualueelle, lukija ja tunniste aloittavat kommunikoinnin. Tavallisesti tunniste kertoo lukijalle oman yksilöidyn tunnistuskoodinsa ja tapauskohtaisesti myös muita siihen ohjelmoituja tietoja. Järjestelmästä riippuen tässä vaiheessa tunnisteelle voidaan myös tallentaa uutta tietoa. (VTT 2004.)

RFID-lukijalaitteet koostuvat kahdesta osasta, antennista sekä itse lukijasta. Antenneja voi olla useampiakin, jolloin saavutetaan esimerkiksi parempi lukualue. Pidemmät lukuetäisyydet saattavat kuitenkin lisätä tunnistintörmäyksiä, eli tilanteita, joissa lukija lukee samaan aikaan useampaa kuin yhtä tunnistinta. Törmäyksistä kerrotaan lisää omassa kappaleessaan. Lukijalaitteet voidaan karkealla jaolla jakaa kahteen pääryhmään, eli kiinteisiin ja kannettaviin. Kiinteitä lukijoita käytetään esimerkiksi varastojen ovilla, tehtaiden liukuhihnoilla (KUVIO 9.) ja varkaudenestosovelluksissa. Porttilukijoita käytettäessä pystytään tunniste lukemaan samanaikaisesti molemmilta puolilta, jolloin luvun onnistumisen todennäköisyys kasvaa. (VTT 2004.)

Kannettavien eli mobiilien lukijoiden (KUVIO 10.) lukuetäisyydet ovat pienen koon ja sitä myötä pienen antennin vuoksi lyhyempiä kuin suuremmilla kiinteillä lukijoilla. Toisaalta sovelluksissa, joissa lukijaa voidaan kantaa helposti mukana, myöskään tarvittavat lukuetäisyydet eivät yleensä ole kovin suuria. Kannettavia käsilukijoita käytettäessä osoitetaan tunnistetta usein samalla tavoin kuin viivakoodia lukiessa ja samaan työprosessiin kuuluu useasti myös tiedon tallennus käsin näppäimistöltä. Paristo- tai akkukäyttöiset käsilukulaitteet toimivat yleensä 13,56 MHz:n alueella. Laitteissa on usein sekä RFID- että viivakoodilukuominaisuudet. (Hämäläinen 2004.)

KUVIO 9. Porttilukija (Jokela 2006.)

KUVIO 10. Kannettava lukijalaite (Nordic ID 2007.)

Halvimmat EPC-standardin mukaiset lukijat maksavat muutamia satoja euroja, ja suurien trukeilla läpiajettavien porttilukijoiden hinnat voivat olla yli 10 000 euroa. Pienet kannettavat laitteet ovat RFID-ominaisuuksiltaan yleensä halvimpia, mutta niissä käytetään usein tiedonsiirtoon langattomia WLAN-yhteyksiä (WLAN, Wireless Local Area Network), jotka nostavat lukijoiden hintoja. Järjestelmien kehittyessä ja tuotantomäärien kasvaessa myös lukijoiden hinnat putoavat. (VTT 2004.)

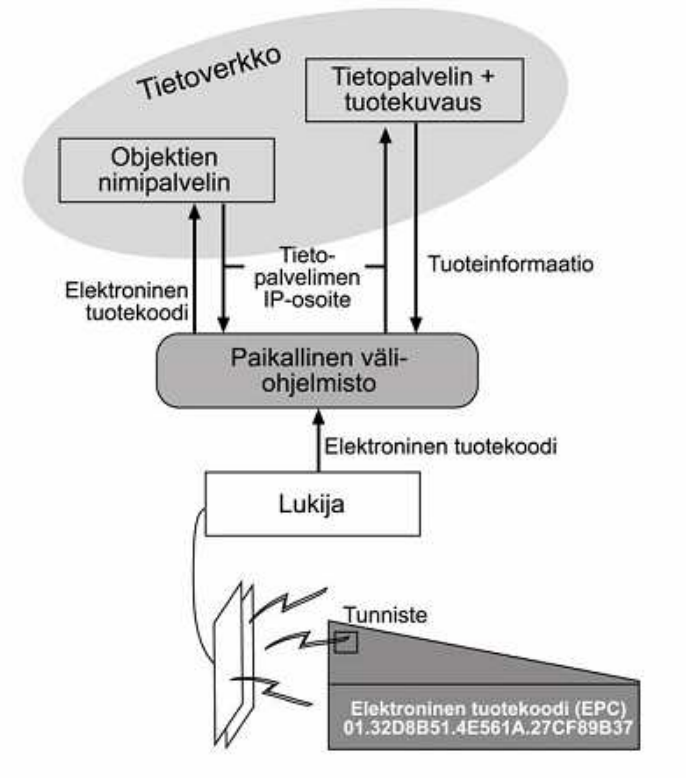
3.3 Tietojärjestelmä

Jotta lukijalaitteen ja tunnisteiden välisestä kommunikoinnista olisi hyötyä, on ne vielä liitettävä tietojärjestelmään, johon varsinainen tieto kootaan ja josta sitä voidaan keskitetysti lukea. Lukijan ja tietojärjestelmän, esimerkiksi kaupan hinta- ja tuotetietokannan välissä toimii yleensä erillinen ohjelmisto, joka käsittelee tietopyynnöt ja ohjaa ne eteenpäin oikeassa muodossa. Ohjelmiston kautta sen käyttäjät pääsevät käsiksi tietokannan sisältöön ja pystyvät siten lukemaan tietoja esimerkiksi yrityksen varaston tilasta keskitetysti yhdestä paikasta – sijaitsivatpa käyttäjät itse missä tahansa.

Tietojärjestelmä on yleensä välttämätön, koska itse tagiin mahtuu hyvin rajallinen määrä tietoa, mutta yrityksen Intranetiin tai Internetiin liitetyssä tietojärjestelmässä tagin tiedot saadaan osaksi suurempaa kokonaisuutta, ja myös

käytettävyys helpottuu. Kun tunnisteet ja tuotteet on kytketty osaksi tietojärjestelmää, voidaan sen kautta hakea lisää tietoa. Haettavan tiedon muoto riippuu aina käyttötarkoituksesta ja käyttäjistä.

Kuviossa 11 on esitetty toimintamalli RFID-lukijan havaitessa tagiin sijoitetun EPC-tuotenumeron. Lukija välittää numeron sovellukselle, joka toimii lukijan ja tietojärjestelmien välissä. Sovellus ottaa yhteyden objektien nimipalvelimeen (ONS, Object Name Service), joka kertoo tuotteen tarkemmat tiedot sisältävän EPC-tietopalvelimen (EPCIS, EPC Information Service) IP-osoitteen. Palvelin sisältää välitettyä EPC-numeroa vastaavat tiedot, kuten tuotteen valmistusajankohdan, kuvauksen ja esimerkiksi missä tuote on edellisen kerran havaittu. Tuoteinformaatio välittyy palvelimelta ohjelmiston kautta haluttuun paikkaan. (VTT 2004.)



KUVIO 11. Tuotetta vastaavien tietojen hakeminen EPC-verkosta (Rintala-Runsala ja Tallgren 2004, 15.)

4 RFID JA RADIOTIEN KÄYTTÖ

4.1 Yleistä radiotaajuuksista

Sähkömagneettinen säteily jaotellaan aallonpituuden mukaan seuraaviin osa-alueisiin: radioaallot, mikroaallot, infrapunasäteily, valo, ultraviolettisäteily, röntgensäteily ja gammasäteily. Tässä opinnäytetyössä käsiteltävät radiotaajuiset tunnistusmenetelmät toimivat radio- ja mikroaaltoalueilla.

Radioaallot ovat sähkömagneettista säteilyä, jonka välityksellä tapahtuu monenlaista tiedonsiirtoa. Esimerkiksi televisio- ja radio-ohjelmat välittyvät radioaaltojen välityksellä jopa maapallon puolelta toiselle. Radioaaltoja käytetään myös muun muassa matkapuhelinverkoissa, radionavigoinnissa ja yhteyksissä avaruusaluksiin. Radioaallot kuljettavat mukanaan energiaa. Langaton tiedonsiirto tapahtuu siten, että lähettäjä sysää liikkeelle sähkömagneettista energiaa, jonka vastaanottaja havaitsee. Molempiin toimintoihin käytetään antenneja, jotka yksinkertaistettuna ovat sähköisiä johtimia. Samaa antennia voidaan käyttää sekä lähettämiseen että vastaanottoon. (Peltonen, Perkkiö & Vierinen 2000, 332–335.)

Taajuusalueet voidaan jakaa luokkiin radioaallon pituuden mukaan (TAULUKKO 2.). Tämänkaltainen jaottelu on kuitenkin epätarkka, sillä esimerkiksi radioaaltojen ja mikroaaltojen rajana pidettävä 1 MHz taajuus on keskellä MF-aluetta. Luetteloa tulisikin käyttää lähinnä ilmaisemaan, minkälaiseen karkeaan luokkaan jokin tietty taajuus kuuluu. Lisäksi taulukolla on yleissivistävä merkitys. (Granlund 2001, 10.)

TAULUKKO 2. Radiotaajuudet (Granlund 2001, 10.)

Aallon pituus	**Taajuus**	**Luokka**
10 km	< 30 kHz	VLF (Very Low Frequency)
1 km	< 300 kHz	LF (Low Frequency)
100 m	< 3 MHz	MF (Medium Frequency)
10 m	< 30 MHz	HF (High Frequency)
1 m	< 300 MHz	VHF (Very High Frequency)
10 cm	< 3 GHz	UHF (Ultra High Frequency)
1 cm	< 30 GHz	SHF (Super High Frequency)
10 mm	< 300 GHz	EHF (Extremely High Frequency)

Kaikki muuttuvassa liikkeessä olevat varaukselliset hiukkaset säteilevät ympäristöönsä sähkömagneettista säteilyä. Radioaallot, kuten muutkin sähkömagneettiset aallot, syntyvät, kun varauksellinen hiukkanen on muuttuvassa liikkeessä synnyttäen sekä muuttuvan magneettikentän että muuttuvan sähkökentän, jotka indusoivat toisiaan. Radioaallot ovat tilassa liikkuvia sähkömagneettisia aaltoja, joiden energia esiintyy sekä sähköisinä että magneettisina kenttinä. Nämä kentät esiintyvät aina yhdessä, sillä muutos sähkökentässä aiheuttaa muutoksen myös magneettikenttään ja päinvastoin. Kun radioaallot etenevät, ne saapuvat lähettäjältä vastaanottajan antennille eri reittejä ja eri voimakkuuksilla. Vastaanottajan antennissa saapuneet aallot summautuvat, ja vastaanotin näkee vain yhden signaalin. Summautumiseen vaikuttavat eri komponenttien keskinäiset vaihe-erot. Vastaanotetun signaalin erot lähetettyyn signaalin nähden riippuvat lopulta siitä, kumoavatko summautuneet komponentit toisensa vai tapahtuuko vahvistus. (Peltonen ym. 2000, 329; Granlund 2001, 11.)

4.2 Radioaallon eteneminen ja vaimeneminen

Radioaalto saavuttaa vastaanottajan, jos hän on lähettimen kuuluvuusalueella. Kuuluvuusalueen kokoon ja muotoon vaikuttavat monet ympäristötekijät, kuten ympäröivät materiaalit ja esteet. Kuuluvuusalueen sisälle saattaa syntyä

katvealueita, joita radiosignaalit eivät syystä tai toisesta tavoita. Kuuluvuusalue voidaan jakaa kolmeen vyöhykkeeseen seuraavasti:

- Alue, jonka sisällä lähettimen signaali kuuluu, ja sen sisältämä informaatio on luettavissa.
- Alue, jonka sisällä lähettimen signaali erottuu taustakohinasta, mutta tietoliikenne ei onnistu huonon yhteyden vuoksi.
- Alue, jonka sisällä lähettimen signaali saattaa häiritä muuta radioliikennettä, mutta sitä ei voida erottaa taustakohinasta.

Viimeksi mainitun alueen ulkopuolella olevalla alueella signaali on niin heikko, ettei se häiritse muuta tietoliikennettä. (Granlund 2001, 12–13.)

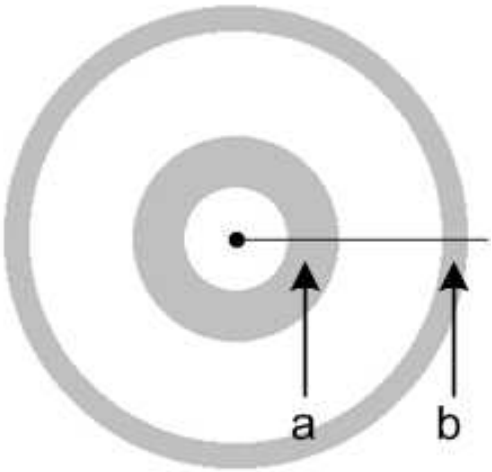
Vaimeneminen tarkoittaa signaalin sisältämän tehon vähenemistä. Sähköjohtimessa signaali vaimenee, koska osa sen tehosta muuttuu resistanssista johtuen lämmöksi. Vaimeneminen ilmenee signaalin amplitudin, eli aallon korkeuden pienenemisenä matkan kasvaessa hävitäkseen lopulta kokonaan. Vaimeneminen ei yleensä vaikuta kaikkiin taajuuksiin tasaisesti, vaan vaimenemisen suuruus vaihtelee taajuudesta ja käytetystä siirtotiestä riippuen. Koska eri taajuudet vaimenevat eri tavalla, tapahtuu vaimenemisen yhteydessä yleensä myös signaalin muodon vääristymistä, jolloin lähetetty signaali saatetaan tulkita vastaanottopäässä väärin. Kokonaisvaimennus lasketaan siirrettävän ja vastaanotetun signaalin suhteena käyttäen yksikköä desibeli (dB). (Granlund 2001, 13.)

$$N = 10\log_{10}(\frac{4\pi d}{\lambda})^2$$

KUVIO 12. Kaava vapaan tilan vaimennuksen laskemiseen

Kaavassa (KUVIO 12.) d kuvaa etäisyyttä ja λ aallonpituutta samassa mittayksikössä. Vaimennus tapahtuu etäisyyden neliössä, eli etäisyyden kaksinkertais-

tuessa vaimennus nelinkertaistuu. Tämä johtuu siitä, että vapaassa tilassa ympärisäteilevä radiosignaali ja sen energia leviävät tasaisesti joka suuntaan (KUVIO 13.). Kuvion renkaat esittävät kuvan keskipisteestä lähetettyä radiopulssia ja renkaan paksuus pulssin tehoa. Kun pulssi etenee lähetyspisteestä kauemmaksi, pulssia edustavan renkaan pituus kasvaa, mutta olemassa oleva teho joudutaan ”venyttämään” pidemmälle matkalle ja rengas ohenee. (Granlund 2001, 13–14.)



KUVIO 13. Ympärisäteilevän radiosignaalin vaimeneminen

Teoriassa signaali etenee äärettömästi, mutta käytännössä sen havaitseminen ja erottaminen taustaäänistä eli kohinasta muuttuu mahdottomaksi jo hyvin rajallisen matkan päässä. Vaimennus on suoraan verrannollinen radioaallon taajuuteen, mistä seuraa, että useita taajuuskomponentteja sisältävä lähetys vääristyy sitä enemmän mitä suuremmaksi etäisyys lähettimestä kasvaa. Tämä johtuu pienempien taajuuskomponenttien suuria voimakkaammasta vaimenemisesta. (Granlund 2001, 13–14.)

4.3 RFID-järjestelmien taajuusalueet

Sovellettava taajuusalue vaikuttaa oleellisesti RFID-järjestelmän toimintaan ja suorituskykyyn. Tunniste ja lukija on suunniteltu keskustelemaan keskenään radioteitse juuri tietyllä taajuudella. Valittu taajuus vaikuttaa muun muassa siihen, toimiiko järjestelmä lähi- vai kaukokentässä, mikä on tiedonsiirtonopeus, millaisia lukuetäisyyksiä järjestelmällä voidaan saavuttaa sekä mikä on tilanne eri maantieteellisillä alueilla taajuusallokoinnin ja tehorajoitusten osalta. Suomessa taajuusalueiden käyttöä kontrolloi Viestintävirasto, joka asettaa rajoitteita ja vaatimuksia myös RFID-laitteistoille. Erilaisia RFID-ratkaisuja on kehitetty useille eri taajuusalueille, mutta monet tekniikat ovat jääneet pienen piirin erikoiskäyttöön muun muassa radioliikenteen sääntelyn kansallisten erojen vuoksi. Maailmanlaajuisesti on päädytty neljälle eri taajuusalueelle: Alle 135 kHz taajuudet, 13,56 MHz taajuudet, UHF-taajuudet (860–930 MHz) sekä mikroaaltotaajuudet (2,45 GHz) (TAULUKKO 3.). Myös VHF-alueelle on olemassa muutamia toteutuksia.

Alle 135 kilohertsin eli matalan taajuuden (LF, Low Frequency) alueella toimivien tunnisteiden tiedonsiirto perustuu magneettikentän indusoivaan käämiin. Taajuus on käytännössä yleensä 125 kHz tai 134 kHz. Tekniikka toimii hyvin metallien lähettyvillä, ja soveltuu siten esimerkiksi metalliesineiden merkitsemiseen, mutta käämin vuoksi tunnisteet eivät voi olla erityisen ohuita. Luettavuus on hyvä myös veden läpi ja läheisyydessä. Koska ihmiset ja eläimet koostuvat paljolti vedestä, matalien taajuuksien RFID-järjestelmiä käytetään paljon kotieläinten merkitsemisessä. Myös kulunvalvontasovellukset ovat yleisiä, logistiikassa LF-alueen toteutukset ovat sen sijaan harvinaisia. Lukuetäisyydet ovat lyhyitä, tavallisesti muutamia senttimetrejä ja korkeintaan noin puoli metriä. LF-alueen tunnisteet ovat passiivisia. (RFID Lab Finland 2007; Kärkkäinen 2006; Top Tunniste 2006.)

Korkean taajuuden (HF, High Frequency) alue tarkoittaa RFID-järjestelmissä käytännössä 13,56 MHz:n taajuutta, joka otettiin laajamittaiseen käyttöön vuosituhannen vaihteessa. Taajuus on vapaasti käytettävissä, sillä se kuuluu kan-

sainväliseen teollisuuden, tieteen ja lääketieteen käyttöön tarkoitettuun ISM-taajuusalueeseen (Industrial, Scientific, Medical). Myös HF-alueen RFID-järjestelmät perustuvat virran indusointiin tunnisteelle, mutta eroavat jonkin verran toiminnallisuuksiltaan LF-järjestelmistä. (Kärkkäinen 2006.)

HF-alueen tunnisteissa antenni on kierretty spiraalimaiseksi johtimeksi, jonka koko riippuu tavoitellusta lukuetäisyydestä. Lukuetäisyydet jäävät tavallisesti alle yhden metrin, usein jopa alle kymmenen sentin. Yleisimpiä käyttökohteita ovat matka- ja kirjastokortit sekä kulunvalvontaan liittyvät sovellukset, joissa etäluettava RFID-tunniste on kätevämpi kuin tarkan kohdistamisen vaatima perinteinen magneettijuovakortti. Tällaisissa käyttöympäristöissä kortti, eli tunniste on yleensä laminoitu muoviin. Rajoittavana tekijänä on tunnisteen toimimattomuus metallin lähettyvillä, mikä saattaa aiheuttaa ongelmia esimerkiksi logistiikassa, jossa käytetään metallisia kuljetusvälineitä. HF-alueen tunnisteet ovat passiivisia. (Hämäläinen 2004; Top Tunniste 2006.)

Tunnisteiden toimivuutta metallipinnoilla voidaan parantaa nostamalla ohut tunniste irti kohteen pinnasta. Mitä korkeammalla tunniste nostetaan, sitä paremmin se toimii. Tunnisteiden korkeus saattaa kuitenkin heikentää niiden käytettävyyttä, joten tunnisteiden korkeus on yleensä alle 10 millimetriä. (VTT 2005.)

UHF-alueella (Ultra High Frequency), eli 860–930 megahertsillä toimivat toteutukset käyttävät lukemiseen yleensä radioaaltoja. Lähiympäristön muilta lukijalaitteilta saapuvien radioaaltojen heijastukset saattavat häiritä lukuoperaatioita aiheuttaen prosessia hidastavia virheitä. Häiriöitä saattavat aiheuttaa myös kännykät ja muut radiolähettimet. Lisäksi tunnisteen taajuuteen vaikuttavat sen kiinnitystapa ja kohteen tiheys, joten tunnisteen kiinnittämiseen ja toimintaympäristöön tulee kiinnittää erityistä huomiota. UHF-taajuuksilla toimivissa tunnisteissa on tyypillisesti jonkin verran ohjelmoitavaa muistia. UHF-taajuuksien järjestelmiä käytetään erityisesti logistiikassa. (Kärkkäinen 2006.)

UHF-alueen RFID-ratkaisut yleistyvät tällä hetkellä kaikkein nopeimmin. Syynä suosioon on ennen kaikkea mahdollisuus käyttää suuntaavia antenneja, jolloin lukuetäisyys paranee huomattavasti, koska tällöin lähetysteho voidaan kohdistaa kapeammalle alueelle. Tähän liittyy kuitenkin myös rajoittava tekijä, eli kansalliset ja kansainväliset lähetystehoja rajoittavat säädökset. Suomessa määräyksistä vastaa Viestintävirasto, joka helpotti vuonna 2005 UHF-alueella toimivien RFID-sovellusten asemaa hyväksymällä muutoksen, jonka mukaan Suomessa voidaan käyttää 2 W teholla toimivia UHF-lukijoita aikaisemman 0,5 W sijasta (Viestintävirasto 2005.). Tyypilliset lukuetäisyydet ovat 2–5 metriä, mutta hyvin optimoiduilla passiivisillakin tageilla voidaan yltää jopa noin 30 metriin. UHF-alueen tunnisteet voivat olla joko passiivisia tai aktiivisia. (Kärkkäinen 2006; Top Tunniste 2006; Kalliokoski 2007.)

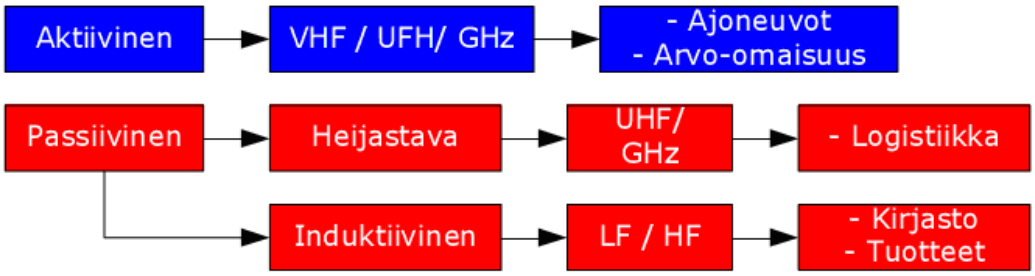
UHF-alueen toteutusten yleistymisen hidasteena on ollut epäselvyys standardeista ja käytettävistä taajuuksista. Asioissa on hiljattain päästy eteenpäin ja Yhdysvalloissa on asetuttu käyttämään taajuuksia 902–928 MHz (915 ± 13 MHz), Euroopassa 865–868 MHz ja Kiinassa 840,25–844,75 MHz sekä 920,25–924,75 MHz. Japanissa jokainen UHF-toteutus vaatii erikseen hyväksynnän maan viranomaisilta. Vaikka yhtenäinen kansainvälinen taajuusalue puuttuukin, standardoinnin myötä kaupallisten sovellusten rakentaminen on turvallisempaa ja vähitellen selkiytyneet säännöt tuovat myös kilpailua, mikä näkyy hintojen alenemisena. (RFID Lab Finland 2007.)

Johtuen perinteisen UHF-tekniikan rajoitteista nesteiden ja metallien läheisyydessä, on UHF-taajuudelle kehitetty myös mahdollisuus lähikenttätunnistamiseen (Near Field UHF). Siinä hyödynnetään UHF-taajuudellakin vallitsevaa noin parinkymmenen sentin lähikenttää, jossa magneettikenttä on vielä riittävän tehokas tunnistamiseen. Lähikenttä-UHF toimii tavallisella UHF-lukijalla ja erityisellä lähikenttäantennilla. (RFID Lab Finland 2007.)

Neljäs maininnan arvoinen RFID-taajuusalue on 2,45 GHz (ISM), jolla toimivat mikroaaltotunnisteet sekä muun muassa Bluetooth, WLAN ja muita lyhyen kantaman sovelluksia (SRD, Short-Range Devices). Taajuusaluetta käytetään erityisesti sovelluksissa, joissa tarvitaan pitkiä lukuetäisyyksiä. Mikroaaltotaa-

juudella toimivien RFID-järjestelmien etu on suuri tiedonsiirtonopeus ja tunnisteiden pieni koko. Mikroaaltotaajuuksilla on käytössä sekä aktiivisia että passiivisia tunnisteita, ja aktiivisilla tunnisteilla voidaan yltää jopa 1 Mbit/s nopeuksiin. Passiivisten mikroaaltotunnisteiden tyypillinen tiedonsiirtonopeus on 10–50 kbit/s. Suurten nopeuksien ansiosta mikroaaltotaajuuksilla toimivat järjestelmät soveltuvat kovallakin vauhdilla liikkuvien tavarayksiköiden, kuten ajoneuvojen, konttien, rekkojen ja junanvaunujen tunnistamiseen. (VTT 2002; Kärkkäinen 2006.)

Korkean taajuutensa vuoksi mikroaaltoja on vaikeampi siirtää kuin matalataajuisia signaaleja. Mikroaaltojen suurimpia haittapuolia on voimakas vaimeneminen. Usein vaaditaan lähes esteetön yhteys lähettimen ja vastaanottimen välillä, jotta yhteys toimii luotettavasti. Mikroaalto vaimenee jopa vesihöyryn vaikutuksesta ja erityisen nopeasti vedessä sekä vettä sisältävässä aineessa.



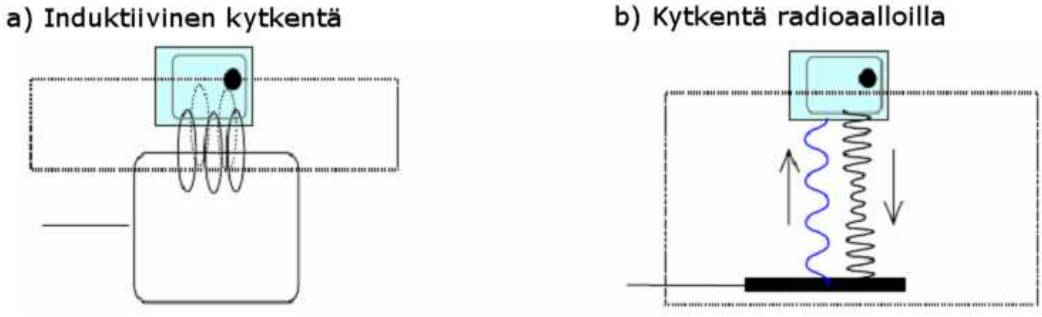
KUVIO 14. Tunnistekartta (ToP Tunniste 2005.)

TAULUKKO 3. Eri taajuuksien RFID-tagien ominaisuuksia (VTT 2004, Kärkkäinen 2006.)

Taajuus	Luku-etäisyys	Käyttöesimerkkejä	Edut	Rajoitteita
LF < 135 kHz	Lyhyt, yleensä alle 0,5 m	Varkaudenestojärjestelmät, kotieläinten merkitseminen	Toimii metallin ja veden lähellä	Lukuetäisyys
HF 13,56 MHz	Lyhyt, yleensä 1 – 1,5 m	Matkakortti-, kirjasto-, kulunvalvonta- ja teollisuuslogistiikka-sovellukset	Hyvin monenlaisia tageja saatavissa, käytetty tekniikka	Tunnistetta ei voi pienentää merkittävästi. Ei toimi metallin lähellä.
UHF 860 – 930 MHz	1 – 10 m	Logistiikka, jakeluketjujen hallinta	Pitkä lukuetäisyys, yleistymässä nopeasti	Vaimenee vedessä tai vettä sisältävässä aineessa.
Mikro-aallot 2,45 GHz	1 – 100 m	Ajoneuvojen etätunnistus	Pitkä lukuetäisyys, tunnisteen pieni koko, vapaa taajuuskaista.	Vaimenee nopeasti vedessä tai vettä sisältävässä aineessa.

4.4 Väliainerajapinta ja kytkeytyminen

Tunniste ja lukijalaite muodostavat toisiinsa fyysisen tason yhteyden kytkeytymällä. Kytkeytyminen tapahtuu väliainerajapinnan kautta tunnisteen ja lukijalaitteen välisen aineen, yleensä siis ilman, välityksellä. Kytkeytyminen voi tapahtua kolmella tavalla: induktiivisesti, kapasitiivisesti tai sähkömagneettisesti. Yleisimmät kytkeytymistavat ovat induktiivinen ja sähkömagneettinen (KUVIO 15.). (Jokela 2006.)



KUVIO 15. RFID-kytkentätyypit (AIM 2005.)

LF- ja HF-taajuusalueita käyttävät tunnisteet toimivat niin sanotussa lähikentässä (induktiivinen kytkeytyminen) ja UHF-tunnisteet puolestaan pääsääntöisesti kaukokentässä (sähkömagneettinen kytkeytyminen). Kun lähikenttä vaihtuu kaukokentäksi, sähkömagneettinen säteily irtoaa antennista muodostaen radioaallon. Lähikenttä on olemassa antennin läheisyydessä ja kaukokenttä kauempana antennista. Lähi- ja kaukokentän karkeana rajana voidaan pitää etäisyyttä $\lambda / 2 \pi$ antennista. (Kuisma 2005b; Jokela 2006.)

Induktiivinen kytkentä liittyy aina johtimen tai piirin muodostamaan silmukkaan. Induktiivisen kytkennän silmukka-antenni indusoi magneettikentän kautta virran tunnisteen silmukkaan. Antenni ja tunniste muodostavat keskenään muuntajan, minkä vuoksi tagin asennolla on vaikutusta lukuetäisyyteen. Kaukokentässä antenni ei indusoi virtaa tunnisteeseen muuntajanomaisesti, vaan tagin tunnistus perustuu radioaaltoihin ja niiden takaisinheijastamiseen (backscatter) tunnisteen dipoliantennista. (RFID Lab Finland 2007, Santanen 2005, Jokela 2006.)

Lähikentästä voidaan erottaa ja mitata erikseen magneetti- ja sähkökentät. Sähkömagneettinen induktio on ilmiö, jossa magneettikentän muutos indusoi, eli saa aikaan sähkövirtaa. Ilmiöön perustuvat muun muassa sähkögeneraattorin, muuntajan ja miinaharavan toiminta. Lähikentän energiasta suuri osa on reaktiivista, eli energia ei säteile ympäristöön eikä se muutu lämmöksi, vaan on dynaamisessa vaikutuksessa antennin kanssa. Lähikentässä laitteen rakenteet, kuten kotelo vaikuttavat läheisyydellään kentän käyttäytymiseen. (Peltonen ym. 2000, 36; Kuisma 2005b.)

Kaukokentässä sähkömagneettisen aallon eteneminen voidaan ajatella tapahtumana siirtää energiaa tai informaatiota kahden pisteen välillä lähettimestä vastaanottimeen. Materiaalin johtavuus määrää häviöt ja sähkömagneettisen aallon vaimenemisen. (Kuisma 2005b.)

Vallitsevat olosuhteet saattavat häiritä kytkeytymistä tai estää sen kokonaan. Vaikka tunnisteen ja lukijalaitteen välille ei yleensä vaadita suoraa näköyhteyttä, voivat ympäristön materiaalit estää magneettivuon ja radioaaltojen etenemi-

sen. Erityisesti tehdasympäristöissä häiriöitä saattavat aiheuttaa erilaiset metallit, jolloin magneettivuon muoto ja voimakkuus muuttuvat. (Jokela 2006.)

Radioaallon osuessa väliainerajapintaan, osa siitä läpäisee rajapinnan ja osa heijastuu takaisin. Heijastuneet säteet aiheuttavat monitie-etenemiseksi kutsutun ilmiön. Monitie-eteneminen tarkoittaa tilannetta, jossa signaali etenee vastaanottimeen useaa eri reittiä esimerkiksi heijastumalla ympäristössä olevista esineistä. Heijastunut signaali saattaa näin ollen kulkea huomattavastikin pidemmän matkan verrattuna lyhimpään reittiin. Heijastuva signaali tulee siis perille ”väärään aikaan”, minkä lisäksi se on heijastumisen yhteydessä menettänyt osan energiastaan. Heijastumiseen vaikuttavat sekä signaalin aallonpituus että aine, josta signaali heijastuu. (Granlund 2001, 16.)

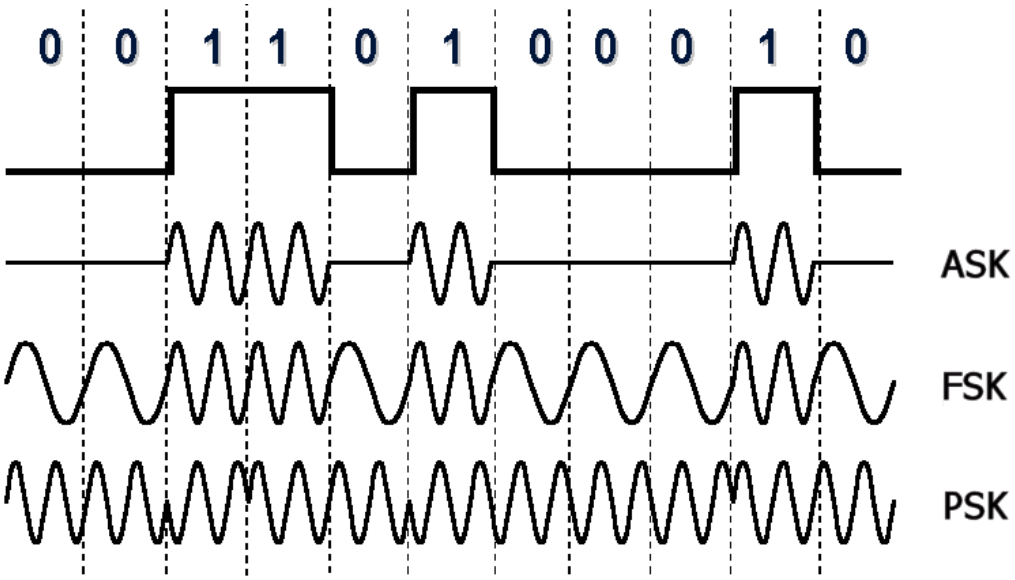
4.5 Modulaatio

Modulaatiolla tarkoitetaan siirrettävän signaalin taajuuden muuttamista toiseksi. Siirtotiellä taajuuden muuttaminen on usein tarpeellista, jotta siitä saataisiin paremmin siirtoon sopiva. Esimerkiksi kun puhetta siirretään radioyhteyden kautta, täytyy alkuperäinen matalataajuinen signaali muuttaa radiotaajuiseksi käytettävän radioyhteyden mukaisesti. Moduloitaessa siirrettävä informaatio liitetään kantoaaltoon. Moduloivaksi signaaliksi sanotaan alkuperäistä siirrettävää signaalia, ja lopputulosta kutsutaan moduloiduksi signaaliksi. Siirron jälkeen signaali yleensä muutetaan takaisin alkuperäiseen muotoonsa demodulaatiolla, joka on modulaation käänteinen toimenpide. Demodulaatiota kutsutaan myös ilmaisuksi (detection). (Kuisma 2005a.)

Modulaation voi suorittaa analogiselle tai digitaaliselle signaalille, mutta RFID-tekniikan luonteen vuoksi seuraavassa esitellään vain digitaalisia modulaatiotekniikoita. Kolme digitaalisen tekniikan perusmuotoa ovat ASK (Amplitude-Shift Keying), FSK (Frequency-Shift Keying) ja PSK (Phase-Shift Keying) (KUVIO 16.). Digitaalinen modulaatio voi tapahtua pääpiirteittäin kahdella tavalla:

- Modulaattorina toimii perinteinen analoginen modulaattori, moduloivana signaalina digitaalinen signaali (esim. pulssijono)
- Modulointi tapahtuu suoraan digitaalisesti prosessoimalla, jonka jälkeen analoginen liityntä RF-rajapintaan

(Kuisma 2005a.)



KUVIO 16. Tavallisimmat digitaaliset modulaatiotekniikat

ASK-modulaatiossa yksittäisiä bittejä tai bittiyhdistelmiä välitetään kantoaallon voimakkuuden, eli amplitudin vaihteluina. ASK on tekniikkana melko tehoton ja altis satunnaisille häiriöille. FSK-modulaatiossa muutetaan kantoaallon amplitudin sijasta taajuutta ja PSK- eli vaihemodulaatiossa moduloiva signaali muuttaa kantoaallon vaihetta.

PSK-modulaatiosta on olemassa eri lajeja, kuten BPSK (Binary Phase-Shift Keying) ja QPSK (Quadrature Phase-Shift-Keying). BPSK käyttää kahta kantoaallon vaihetta ilmaisemaan digitaalista nollaa tai ykköstä, esimerkiksi 0 ja +180 astetta. QPSK sen sijaan käyttää neljää kantoaallon vaihetta, esimerkiksi 0, +90, +180 sekä + 270 astetta ja voi ilmaista kerralla kaksi bittiä; 00, 01, 10 tai 11.

4.6 Törmäystenhallinta ja kanavointi

4.6.1 Yleistä törmäystenhallinnasta

Usein tulee tarve viedä monia RFID-tunnisteita samanaikaisesti lukijalaitteen läpi. Tällaisia tilanteita voi tulla esimerkiksi lastausvarastoissa, joissa isoja tavaraeriä liikutellaan tiiviisti pakatuilla lavoilla, jotka halutaan merkitä saapuviksi tai lähteviksi. Kun tunnistein merkityt tuotteet tuodaan lukijan kenttään, kaikki tunnisteet aktivoituvat ja lähettävät tietonsa samaan aikaan, mikä aiheuttaa lukijalle ongelmia yhtäaikaisen liikenteen hallitsemisessa. Syntyy muussakin tietoliikenteessä tavattavia törmäyksiä, eikä kaikki lähetetty tieto saavu perille, koska lukijan on mahdotonta erottaa samaan aikaan tulevia tunnisteiden lähetyssignaaleja toisistaan. (Spurgeon 2001.)

Törmäyksiä on lähes mahdotonta välttää kokonaan, mutta niiden havaitseminen on oleellista, jotta tieto voidaan tarvittaessa lähettää uudelleen. Ongelman ratkaisemiseksi on kehitetty erityisiä menetelmiä, joiden avulla törmäyksiä pyritään joko vähentämään tai havaitsemaan. Menettelytavat vaihtelevat laitevalmistajista ja käyttökohteista riippuen. On esimerkiksi olemassa protokollia, jotka huolehtivat, että kaikki halukkaat saavat vapaan lähetyshetken yhteisen jaetun median (shared medium) käyttöön. RFID:n tapauksessa jaettuna mediana voidaan pitää lukijalaitetta tai ilmarajapintaa. Törmäystenhallintaan kehitetyt protokollat eivät ole uusi keksintö, vaan niitä on käytetty tiedonsiirrossa jo pitkään. Mekanismia kutsutaan kilpavarausmenetelmäksi (contention-based), jonka parhaiten tunnettu käyttökohde on Ethernet. (Spurgeon 2001.)

Yksi keino välttää ylimääräisiä törmäyksiä ja tehostaa siirtotien käyttöä on kanavointitekniikan käyttäminen. Kanavointi tarkoittaa, että yhteistä siirtotietä käytetään useaan yhtäaikaiseen liikennöintiin. Usein järjestelmät käyttävät kerrallaan vain murto-osan koko siirtotien kapasiteetista, joten ei ole järkevää varata koko kanavaa yhdelle lähetteelle. Kanavoinnilla saavutettavia hyötyjä ovat ennen kaikkea siirtonopeuden kasvu ja käyttöasteen eli tehokkuuden parantuminen. Kun useita lähetteitä liitetään samalle siirtotielle, toimenpidettä kutsutaan multipleksoinniksi (multiplexing). Vastaanottopäässä tapahtuva

käänteinen toimenpide on demultipleksointia (demultiplexing). Yksi mahdollisuus törmäysten välttämiseen on käyttää jokaisella asemalla omaa taajuusaluetta siten, että jaetut taajuudet eivät mene päällekkäin. Tekniikka on nimeltään Frequency Division Multiplexing (FDM). Toteutus on kuitenkin monimutkainen ja jos laitteita on useita, taajuusalueet loppuvat nopeasti kesken. Juuri taajuuksien riittämättömyyden vuoksi taajuusjakoinen tekniikka sopii vain tietynlaisiin pienempiin ympäristöihin. (Laynetworks 2007.)

Toinen RFID-tekniikassa käytetty kanavointimenetelmä on aikajakokanavointi (TDM, Time Division Multiplexing), jossa jokaiselle asemalle varataan taajuuden sijasta oma aikajakso eli aikaväli. TDM:n käyttöönotto on helpompaa, koska voidaan keskittyä käyttämään yhtä taajuusaluetta koko järjestelmässä. Tekniikka ei kuitenkaan ole kovin tehokas, koska jos tietylle asemalle varatut aikajaksot jäävät käyttämättä, mikään muukaan asema ei voi niitä hyödyntää ja potentiaalista siirto- ja lähetysaikaa menee hukkaan. Aikaväleihin perustuu myös Slotted ALOHA -tekniikka, jota käytetään älykorttien yhteydessä.

4.6.2 Tunnistintörmäys ja lukijatörmäys

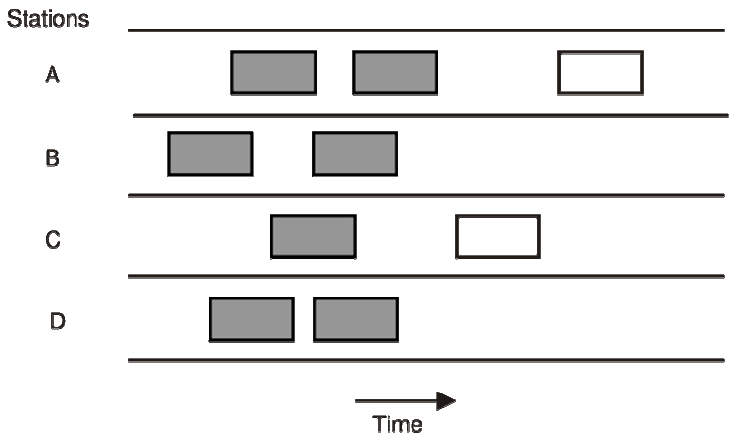
RFID-järjestelmissä on olemassa pääasiassa kaksi erilaista törmäystä. Tunnistintörmäys (tag collision) tapahtuu kun useat tunnisteet tulevat lukijan kenttään ja lähettävät omat signaalinsa lukijalle samanaikaisesti, jolloin lukijan on mahdotonta erottaa samaan aikaan lähettäviä tageja toisistaan. Ongelmaa ilmenee suuria tavaraeriä käsiteltäessä. Tunnisteiden tulisi lähettää tietonsa hieman eri aikoihin, jotta lukija pystyisi onnistuneesti lukemaan ja tulkitsemaan ne kaikki. (Christensen 2007.)

Lukijatörmäys (reader collision) saattaa syntyä mikäli kahden tai useamman lukijalaitteen kantoalueet ovat osittain päällekkäiset. Päällekkäisyydestä voi seurata kahdenlaisia ongelmia. Lukijat saattavat lukea samaa tunnistinta, jolloin sen tiedot voivat tallentua järjestelmään tahattomasti useammin kuin kerran. Tallennusvaiheessa tulisikin aina varmistaa, ettei luettua tunnistetta ole luettu jo aikaisemmin saman istunnon aikana. (Christensen 2007.)

Toinen mahdollinen ongelma on lukusignaalien välinen interferenssi, jolloin signaalit häiritsevät toisiaan. Ongelma on ratkaistavissa lukijoihin ohjelmoitavalla ajastuksella, jolla laitteet voidaan asettaa tekemään lukuoperaationsa hieman eri aikoihin. Päällekkäiset signaalit voidaan välttää säätämällä lukijoiden lähetystehoja. Pienemmällä teholla saadaan aikaan pienempi lukualue ja jos käyttöympäristö pysyy samana, voidaan tehot optimoida sen mukaisesti. (Christensen 2007.)

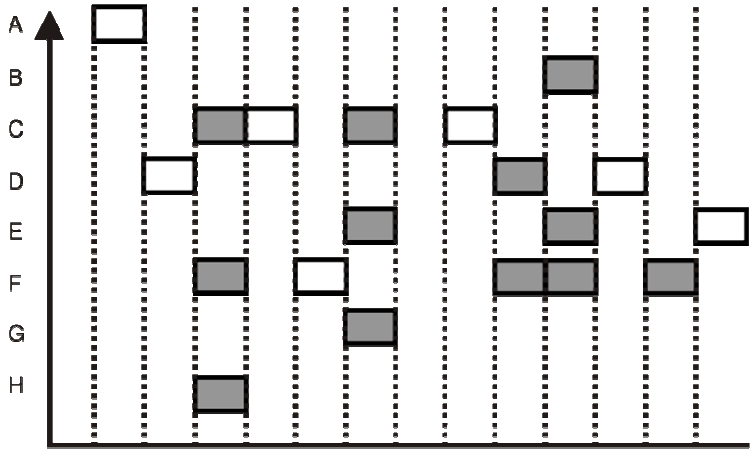
4.6.3 Slotted ALOHA

Yksi RFID-maailmassa törmäysten välttämiseksi käytetyistä tekniikoista on Slotted ALOHA, jota sovelletaan muun muassa muutamissa älykorttitoteutuksissa. Slotted ALOHA on kehittynyt 60- ja 70-luvuilla syntyneestä Pure ALOHA -menetelmästä. Pure ALOHA -verkossa asemat lähettävät heti kun niillä on jotain lähetettävää, eli minkäänlaista kuuntelua ennen lähetystä ei suoriteta (KUVIO 17.). Tämän jälkeen asema jää odottamaan vastaanottajan kuittausta, ja mikäli kuittausta ei tule, lähetetään sanoma uudelleen satunnaisen ajan kuluttua. (Laynetworks 2007.)



KUVIO 17. Tummat kuviot kuvaavat törmäyksiä, jotka ensimmäisissä ALOHA-järjestelmissä olivat hyvin yleisiä

Pure ALOHA -toteutuksessa törmäysten todennäköisyys on suuri, joten niiden vähentämiseksi ryhdyttiin kehittämään parempaa menetelmää. Syntyi Slotted ALOHA, jossa kanava on jaettu tietynkokoisiin aikaväleihin (timeslot), ja kukin asema voi lähettää vain tiettyjen aikavälien aikana (KUVIO 18.). Jokaisen välin pituus on aika, joka tarvitaan yhden paketin lähetykseen. Lähetykset aloitetaan aina aikajakson alussa. Jos kanavalla sattuu törmäys, se on täydellinen ja siten Slotted ALOHA:n hyötysuhde on parempi kuin Pure ALOHA:n. Mikäli aikavälissä tapahtuu törmäys, jokainen tuolloin lähettävänä ollut asema uudelleenlähettää pakettinsa satunnaisen ajan kuluttua. (Laynetworks 2007.)



KUVIO 18. Slotted Aloha -järjestelmä ja aikavälit, tummat kuviot kuvaavat törmäyksiä

4.7 Koodaus

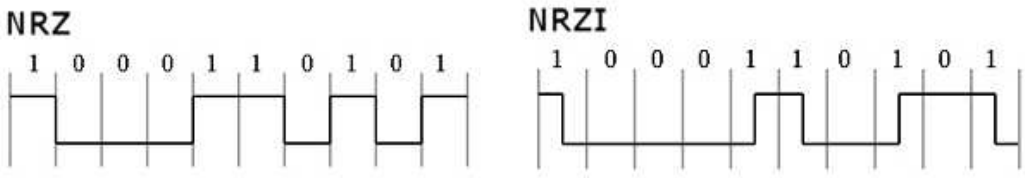
4.7.1 Yleistä koodauksesta

Tietoliikenteessä linjakoodausta hyödynnetään tiedon siirrossa siirtotiellä. Koodaamalla tieto ennen lähetystä, saadaan koodaustavasta riippuen esimerkiksi lisättyä tiedonsiirtonopeutta tai vähennettyä tiedonsiirrossa tapahtuvien virheiden todennäköisyyttä.

RFID-järjestelmissä käytetään muun muassa NRZ-, Manchester- ja Miller-koodauksia. Nämä menetelmät on esitelty seuraavissa kappaleissa.

4.7.2 NRZ-koodaus

NRZ (Non-Return to Zero) on hyvin yksinkertainen menetelmä bittivirran koodaamiseen. Ykkösellä käytetään korkeampaa jännitetasoa ja nollalla matalampaa. Ongelmana ovat pitkät nolla- ja ykkössarjat, joiden aikana tahdistus helposti katoaa. Lisäksi pitkän nollasarjan erottaminen elottomasta yhteydestä voi olla vaikeaa (KUVIO 19.). Ykkössarjojen ongelmaan on kehitetty ratkaisu, joka on nimeltään NRZI (Non-Return to Zero Inverted). Siinä jännite vaihtuu jokaisella ykkösellä, mutta nollasarjaongelmaa sekään ei korjaa. (Shepard 2005, 78–-84.)

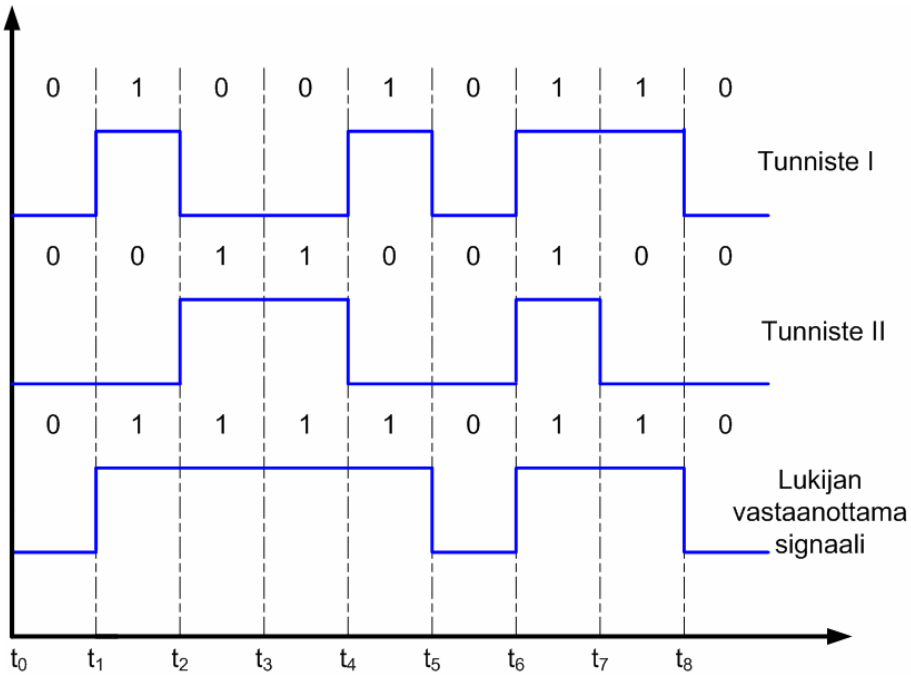


KUVIO 19. Sama bittijono NRZ- ja NRZI-koodattuna

Kuvitellaan tilanne, jossa yksi tai useampi saman lukijan lukualueella oleva tunniste lähettää signaalinsa samanaikaisesti. Lukijamme vastaanottaa lähetteen ja tulkitsee sen ykköseksi. NRZ-koodausta käyttämällä on kuitenkin mahdotonta sanoa onko signaali tullut yksittäiseltä tagilta vai joukolta tunnisteita, joiden suorittamat lähetteet ovat mahdollisesti yhdistyneet samanaikaisuuden vuoksi. Lukijan kannalta tilanne on selkeä, koska se on vastaanottanut vain yhden signaalin ja voi tulkita vain sen ilman tietoa muista. RFID-järjestelmä sen sijaan saattaa toimia hyvin vajavaisesti, jos joukko tunnisteita jää lukematta. Jos käyttöympäristössä on tarpeellista lukea useampia tunnisteita samanaikaisesti, ei NRZ-koodauksen käyttöä voi suositella. (Shepard 2005, 78–84.)

Kuvio 20. esittää tilannetta, jossa Tunniste I lähettää NRZ-koodatun bittivirran ”010010110” ja samanaikaisesti Tunniste II lähettää bittisarjan ”001100100”. Lukijan vastaanottama signaali on näiden kahden tunnistimen lähettämän signaalin looginen summa ”011110110”, joka ei muistuta kumpaakaan lähetetyis-

tä signaaleista, eikä siitä myöskään voida muodostaa kumpaakaan niistä. On siis tapahtunut törmäys, jonka seurauksena molemmat lähetetyt signaalit on menetetty. Suurempi ongelma on kuitenkin se, että NRZ-koodauksen puutteista johtuen tapahtunutta törmäystä ei mitenkään pystytä todentamaan ja tunnistettavaksi tarkoitetut tuotteet saattavat hetken kuluttua jo olla lukijan ulottumattomissa. Tarvitaan siis parempi koodausmenetelmä. (Shepard 2005, 78–84.)



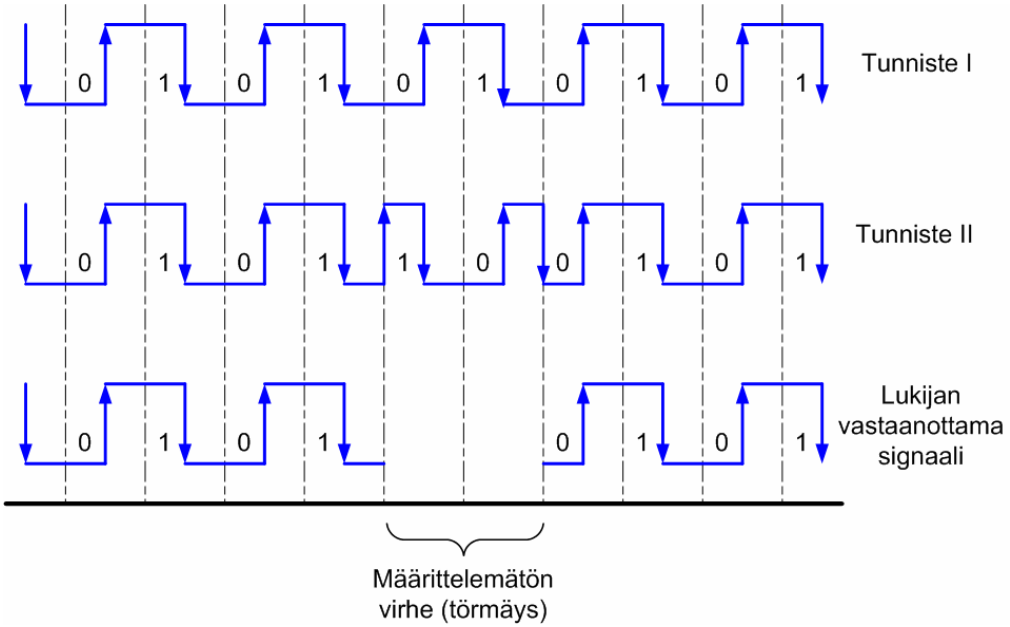
KUVIO 20. Esimerkki, jossa samanaikaisesti lähetettyjä NRZ-koodattuja signaaleja ei pystytä erottamaan toisistaan eikä törmäystäkään voida havaita

4.7.3 Manchester- ja Miller-koodaukset

Manchester-koodauksessa muutos tapahtuu aina bitin puolivälissä toisin kuin tavallisessa NRZ-koodauksessa, jossa jännitetaso (nolla tai ykkönen) säilytetään koko bitin ajan. Manchesterissa nollalla noustaan alhaalta ylös ja ykkösellä pudotaan ylhäältä alas. Menetelmän vahvuus on siinä, että vaikka bittivirta pysyisi yhtäjaksoisesti samana useammankin bitin ajan, koodatussa signaalissa tapahtuu silti aina muutos jokaisella bitillä. Näin pystytään tunnistamaan missä

kohdassa esimerkiksi nollabitti muuttuu toiseksi nollabitiksi, eikä niitä tulkita virheellisesti yhdeksi ja samaksi. (Shepard 2005, 83–86.)

Manchester-koodausta käyttämällä törmäykset voidaan tunnistaa (KUVIO 21.). Esimerkissä kaksi tunnistetta lähettää samanaikaisesti toisistaan eroavat bittisarjat ”0101010101” ja ”0101100101”. Tuloksena summautuu signaali, joka ei noudata Manchester-koodauksen sääntöä, jonka mukaan jokaisella bitillä pitäisi tapahtua muutos. Niinpä lukijan toimintalogiikka havaitsee törmäyksen tapahtuneen ja osaa pyytää uudelleenlähetystä.



KUVIO 21. Esimerkki, jossa lukija havaitsee Manchester-koodattujen signaalien törmäyksen

Miller-koodaus tunnetaan myös nimellä Delay Encoding. Se on selvästi kahta aiemmin esiteltyä harvinaisempi, mutta silläkin on omat käyttökohteensa. Miller-koodaus toimii siten, että 1-bitillä muutos tapahtuu jakson keskellä ja 0-bitillä toimenpide riippuu seuraavasta bitistä. Mikäli nollan jälkeen tulee ykkönen, muutosta ei tapahdu, mutta kahdella perättäisellä nollalla suoritetaan muutos bitin lopussa. (Peuhkuri 1996.)

4.8 Tunnisteen valintaprosessi

Lukijan on valittava yksi tunniste kerrallaan, jonka kanssa kommunikoida. Tässä kappaleessa on esitelty ISO 14443 -standardin A-tyypin kortinvalintamenettely (ks. kappale 5.4), koska se soveltuu hyvin yleismaalliseksi esimerkiksi aiheesta. Menetelmä toimii samalla oleellisena osana törmäystenhallintaa ko. standardissa.

Valintamenetelmä perustuu tunnisteiden sarjanumeroihin. Jokaisella tunnisteella on oma sarjanumeronsa, jonka tulee olla uniikki omalla käyttöalueella. Sarjanumeron ei siis välttämättä tarvitse olla ainutkertainen koko maailman mittakaavassa, mutta yksittäisen järjestelmän tehokkaan toimimisen kannalta on suotavaa, ettei saman järjestelmän piirissä ole kahta tai useampaa samalla sarjanumerolla merkittyä tagia. Useimmiten sarjanumerot ovat vähintään 32-bittisiä, jolloin mahdollisia kombinaatioita on kaikkiaan lähes 4,3 miljardia kappaletta (2^{32} = 4 294 967 296). (Shepard 2005, 83–86.)

Valintamenetelmä perustuu neljään lukijan tuottamaan komentoon:

- REQUEST_SNR: Kyselymäinen komento, joka sisältää sarjanumeron. Jos tunnisteen sarjanumero on sama tai pienempi kuin lukijan lähettämässä komennossa vastaanotettu sarjanumero, tunniste vastaa omalla sarjanumerollaan. Vaikka oikea tunniste ei heti löytyisikään, pystytään komennon avulla rajaamaan potentiaalisten oikeiden tunnisteiden joukkoa.

- SELECT_SNR: Komento, joka valitsee juuri tietyn tunnisteen. Komento sisältää sarjanumeron, ja jos se on sama kuin tunnisteen sarjanumero, tunniste siirtyy valmiustilaan (READY state) odottamaan seuraavia komentoja. Jos sarjanumerot eivät täsmää, tunniste siirtyy odotustilaan, jossa se hyväksyy vain REQUEST_SNR-komennon.

- READ_DATA: Vastaanotettuaan tämän komennon tunnistin lähettää omat tietonsa lukijalaitteelle.

- UNSELECT: Keskeyttää kaiken toiminnon kyseisen tunnisteen kanssa asettaen sen Idle-tilaan, jolloin se ei vastaa edes REQUEST_SNR-kyselyihin. Näin pystytään varmistamaan muille tunnisteille suurempi toimintaprioriteetti toimintahetkellä. Jotta tunnistetta voitaisiin taas käyttää, se täytyy ensin viedä pois lukijan kentästä, eli sen virransaanti tulee katkaista.

(Shepard 2005, 86–87.)

Jos esimerkiksi järjestelmässä käytetään 8-bittisiä sarjanumeroita ja REQUEST_SNR-komento lähettää suurimman mahdollisen bittiarvon eli ”1111 1111”, tällöin kaikki kantoalueella olevat tunnisteet vastaavat lukijalle kukin omalla sarjanumerollaan. Näin lukija voi saada tietoonsa tunnisteiden lukumäärän. Oletetaan, että tunnisteita on kolme (T_1-T_3) ja niillä on seuraavat 8-bittiset sarjanumerot (KUVIO 22.).

T_1	0	1	0	0	1	1	0	1
T_2	0	1	0	0	1	1	1	0
T_3	0	1	0	0	1	1	1	1
Bitti:	7	6	5	4	3	2	1	0

KUVIO 22. Kolmen tunnisteen sarjanumerot ja bittipositiot

Esimerkin järjestelmässä lukijan ja tunnisteiden välisessä tiedonsiirrossa käytetään Manchester-koodausta, minkä ansiosta lukija kykenee tunnistamaan törmäyskohdat ja pystyy tarvittaessa keskeyttämään tiedonsiirron yksittäisten häiritsevien tunnisteiden kanssa. Esimerkkitapauksessa haitalliset törmäykset tapahtuvat bittipositioilla nolla ja yksi muiden bittien ollessa kullakin tunnis-

teella keskenään täsmälleen samat. Törmänneistä biteistä merkitsevin on bittipositioltaan yksi, eli toinen bitti oikealta luettuna. Tästä lukija voi päätellä, että luettavia tunnisteita on vähintään kaksi kappaletta. (Shepard 2005, 87–88.)

Kun törmäys havaitaan, lukija ryhtyy karsimaan samanaikaisesti lähettävien tunnisteiden määrää käyttämällä edellä esiteltyjä komentoja. Vastaavasti myös jo lähetyksensä tehneet tunnisteet asetetaan tilaan, jossa ne eivät enää voi häiritä yhä liikennöiviä tageja. Lukijan on huolehdittava, että kaikki tunnisteet tulevat varmasti luetuksi. Lukijalaitteen oman ohjauslogiikan ja tekoälyn toiminta ovat oleellisia osatekijöitä onnistuneessa lukuprosessissa erityisesti, kun on kyse suurista tunnistemääristä. (Shepard 2005, 87–88.)

4.9 Virheenkorjaus

Kaikenlainen tiedonsiirto on altis virheille. Digitaalisessa tiedonsiirrossa virhe on yksinkertainen: yksittäisen bitin arvon muuttuminen tarkoituksettomasti nollasta ykköseksi tai päinvastoin. Mitä enemmän liikennettä siirtyy, sitä suuremmaksi muodostuu virheen todennäköisyys. Virheitä tapahtuu, mutta oleellista on huomata ja korjata ne. Virheiden havaitsemiseen on ajan saatossa kehitetty erilaisia menetelmiä, RFID:n yhteydessä käytetään usein CRC-tarkistussummaa (Cyclic Redundancy Check). Tehokkuutensa ansiosta CRC on tietotekniikan käytetyin virheiden havaitsemiseen soveltuva menetelmä. (Freeman 1999.)

Tarkistussummaan perustuvassa virheenkorjauksessa lasketaan jakojäännös lähetetystä datasta ja liitetään tarkistussumma yleensä lähetteen loppuun. Kun vastaanottaja on vastaanottanut datan sekä tarkistussumman, se laskee datasta oman tarkistussummansa samalla menetelmällä kuin lähettäjä ja vertaa sitä vastaanotettuun tarkistussummaan. Jos summat vastaavat toisiaan, voidaan olettaa, että tieto on siirtynyt virheittä. Muussa tapauksessa pyydetään yleensä uutta lähetystä. (Freeman 1999.)

CRC:ssä tarkistusbitit generoidaan jakamalla sanoman bittijono muodostajapolynomilla ja sijoittamalla tarkistusbiteiksi saatava jakojäännös. CRC:ssä esimerkiksi kahdeksan tavun merkkijonoa käsitellään 64 bitin lukuna. Muodostajapolynomin pituudella pystytään määrittämään kuinka monta virhettä menetelmällä kyetään havaitsemaan. CRC-tarkistussumman tehokkuus riippuu lähinnä käytettyjen bittien lukumäärästä. Käytännössä kahdeksan bitin CRC:llä havaitaan yli 99,9 % ja 16 bitillä jo yli 99,99 % virheistä. (Freeman 1999.)

5 KONTAKTITTOMAT ÄLYKORTIT

5.1 Yleistä älykorteista

Älykortit ovat tavallisesti muovisia kortteja, joihin on sisällytetty elektroniikkaa erilaisia käyttötarkoituksia varten. Esimerkiksi nykyiset pankki- ja luottokortit on toteutettu tällaisella sirutekniikalla (KUVIO 23.), joka käytettäessä vaatii fyysisen kontaktin lukijalaitteen ja kortin välille. (Shepard 2005, 70–72.)

KUVIO 23. Perinteinen sirukortti (Alpha Card 2007.)

Uudet älykortit ovat yksi merkittävä RFID-tekniikan käytännönsovellus. Radiotaajuustunnistuksen ansiosta uudet kontaktittomat kortit eivät enää vaadi fyysistä kontaktia lukijalaitteisiin. Sen sijaan riittää, että kortti on esimerkiksi muutaman senttimetrin etäisyydellä lukijasta, minkä ansiosta kortin käyttö on nopeampaa ja helpompaa esimerkiksi bussissa tai yleisötapahtumassa korttia lompakosta kaivamatta. Lukuetäisyydet riippuvat järjestelmästä ja käytetystä standardista. RFID-älykortteja käytetään Suomessa jo muun muassa pääkaupunkiseudun joukkoliikenteessä. Samaa tekniikkaa käytetään myös uusissa biopasseissa (kappale 6.1). (Shepard 2005, 70–72.)

5.2 Älykorttien standardit

Vuonna 1998 ISO (International Organization for Standardization) ja IEC (International Electrotechnical Commission) perustivat ISO/IEC JTC1 (Joint Technical Committee on International Technology) -toimikunnan, joka koostuu 20 pienemmästä toimikunnasta informaatioteknologian eri aloilta. Näistä SC17 (Subcommittee 17) sai tehtäväkseen henkilötunnistukseen ja tunnistuskortteihin liittyvien standardien kehittämisen. Standardeissa määritellään esimerkiksi testausmenettelyt sekä vaaditut ominaisuudet ja niiden toiminnallisuus muun

muassa magneettinauhakorteille, kontaktittomille älykorteille sekä koneella luettaville matkustusdokumenteille kuten passeille ja ajokorteille. Lisäksi määritellään kortille vaaditut sietokyvyt muun muassa ultraviolettivalolle, röntgensäteille, taivutus- ja kiertoliikkeille, sähkö- ja magneettikentille sekä lämpötiloille. (Shepard 2005, 70.)

SC17:llä on useita työryhmiä (WG, working group), joille vastuu tunnistustekniikoista on jaettu seuraavasti:

- WG1: Fyysiset ominaisuudet ja testausmenettelyt
- WG3: Koneluettavat matkustusdokumentit
- WG4: Kontaktilliset sirukortit
- WG5: Rekisteröintien hallinta
- WG7: Rahaliikennekortit, luottokortit
- WG8: Kontaktittomat älykortit sekä niihin liittyvät laitteet ja liitynnät
- WG9: Optiset muistikortit sekä niihin liittyvät laitteet ja liitynnät
- OWG (Operating Working Group): Tekniikoiden yhteiskäyttö ja tunnistuskortit
- WG10: Ajokortit

(Shepard 2005, 71.)

WG8 vastaa kontaktittomista älykorteista, joita kutsutaan myös nimellä ID-1. Kontaktittomat älykorttiratkaisut on standardoitu seuraavasti:

- ISO 10536: Lyhyen kantaman kortit (CICC, Close-coupling Integrated Circuit Cards)
- ISO 14443: Lähilukukortit (PICC, Proximity Integrated Circuit Cards), jakautuu A- ja B-tyypin kortteihin
- ISO 15693: Etälukukortit (VICC, Vicinity Integrated Circuit Cards)

(Boussouira 2002.)

Seuraavissa kappaleissaan esitellään kolmen yllä mainitun standardin korttitoteutuksia ja niiden toimivuutta. Kappaleissa keskitytään lähilukukortteihin

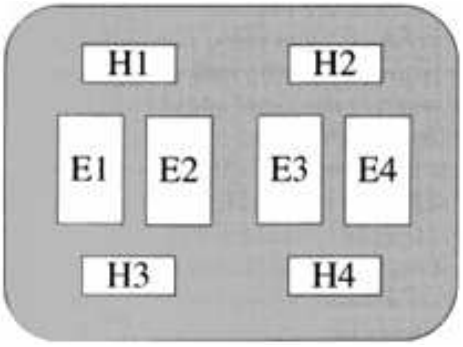
(ISO 14443) niiden suhteellisen yleisyyden vuoksi. Standardista ovat kiinnostuneet myös suuret elektroniikka-alan yritykset kuten Philips, joka on luonut siihen pohjautuvan oman toteutuksensa.

Philips on kehittänyt ja lisensoinut ISO 14443A -standardiin perustuvan MIFARE-älykorttiteknologian. MIFARE:n pääasiallisia käyttökohteita ovat julkisen liikenteen ja erilaisten tapahtumien elektroniset pääsylippujärjestelmät. MIFARE:n Internet-sivustolla www.mifare.net kerrotaan piirejä myydyn yli 500 miljoonaa ja lukijoita viisi miljoonaa kappaletta. Teknologia on yhteensopiva ISO 14443A -standardin kanssa lukuun ottamatta tiedonsiirtoprotokollaa, joka on Philipsin itsensä kehittämä.

5.3 Lyhyen kantaman kortit

ISO 10536 -standardin mukaisten lyhyen kantaman korttien (CICC) lukuetäisyydet ovat erittäin lyhyet, korkeintaan yhden senttimetrin luokkaa. Käytännön toteutuksissa on usein fyysinen kontakti kortin ja lukijan välillä. Lyhyen lukuetäisyyden vuoksi kortteja käytetään lähinnä sellaisten lukijoiden kanssa, joissa on aukko kortin syöttämistä varten. Tällaisia ratkaisuja voi nähdä esimerkiksi kortilla avattavissa hotellihuoneiden ovissa. (Shepard 2005, 70–72.)

Koska lukuetäisyydet ovat hyvin lyhyitä, täytyy lukijalaitteen ja kortin lukupinnan osua tarkasti kohdakkain, jotta lukuoperaatiot voivat onnistua. Korttiin on sijoitettu induktiivisia ja kapasitiivisia komponentteja, joiden sijainnit on tarkasti määrätty standardissa, jotta varmistetaan kortin mahdollisimman hyvä luettavuus eri lukuasennoissa (KUVIO 24.). (Shepard 2005, 71–73.)



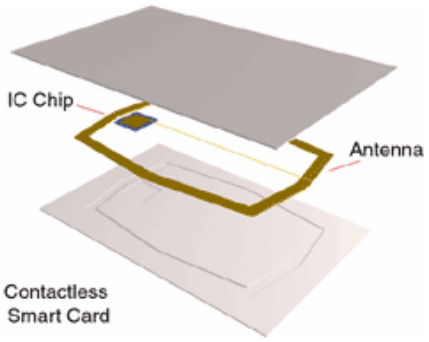
KUVIO 24. CICC-kortin komponenttien sijoittelu (Shepard 2005.)

Kortin induktiiviset komponentit tuottavat kortin vaatiman virran generoimalla muuttuvan sähkökentän (4,9152 MHz). Kuvan käämit H1 ja H2 on kierretty päinvastaisesti kuin käämit H3 ja H4, jolloin niihin yhtäaikaisesti syötetty virta aiheuttaa magneettikenttien välille 180 asteen vaihe-eron. Näin saadaan aikaan noin 200 milliwatin kokonaisteho. Tiedonsiirto voi olla induktiivista tai kapasitiivista, mutta tyyppi ei voi muuttua kesken tiedonsiirron. (Shepard 2005, 72–74.)

5.4 Lähilukukortit

5.4.1 Yleistä lähilukukorteista

ISO 14443 -standardin määräysten mukaiset lähilukukortit (PICC) on suunniteltu toimimaan noin 10 - 25 senttimetrin etäisyydellä lukijalaitteesta. Tyypillisiä käyttökohteita ovat esimerkiksi kirjasto-, matka- ja kulunvalvontakortit. Standardi määrää korttien mitoiksi samat kuin perinteisille kontaktikorteille (ISO 7810); 3,37 x 2,12 tuumaa, paksuus 0,03 tuumaa. Lisäksi tässäkin standardissa määritellään jo aikaisemmin mainitut sietokyvyt muun muassa ultraviolettisäteilylle ja kortin taivutuksille. (Shepard 2005, 76–77.)



KUVIO 25. Kontaktittoman RFID-älykortin rakenne (Alpha Card 2007.)

KUVIO 26. Esimerkki lähilukukortista (Alpha Card 2007.)

RFID-standardien kehityksen alkutaipaleella niiden kehityssuunnasta esiintyi laajaa erimielisyyttä. ISO 14443 -standardin osalta tämä johti kahden erillisen standardin syntymiseen: ISO 14443 Type A ja ISO 14443 Type B. Lähes poikkeuksetta lähilukukortit tukevat vain jompaakumpaa, mutta korttien lukijoiden (PCD, Proximity Coupling Device) on tuettava molempia standardeja. Eroavaisuudet liittyvät lukijoiden ja korttien tapaan keskustella keskenään. A- ja B-tyypit eroavat toisistaan magneettikentän modulointitavan, bittiesitystavan ja koodauksen sekä törmäyksenhallinnan osalta. Erot eivät käytännössä näy tavalliselle käyttäjälle, mutta suunnittelijoiden kannalta toteutustavat ovat hyvin erilaiset. (Shepard 2005, 76–77.)

5.4.2 Teho- ja signaalirajapinta

Lukijalaitteen ja kortin välinen vuoropuhelu on pääpiirteissään yksinkertaista ja hyvin samanlaista sekä A- että B-korttityypeillä. Kun kortti saapuu lukijalaitteen radiokenttään, se aktivoituu ja jää odottamaan komentoa lukijalta. Kun lukijalaite tahtoo kommunikoida kantoalueella olevan kortin kanssa, se lähettää komennon, johon kortti puolestaan vastaa. Tehon tuottaminen on lukijalaitteen tehtävä. Lähilukukortit saavat energiansa lukijalaitteen muodostamasta vaihtuvasta magneettikentästä, jonka taajuus 13,56 MHz ± 7 kHz on sama molemmil-

le korttityypeille. Magneettikentän voimakkuus on 1,5–7,5 A/m. Sekä A- että B-tyypin korteilla tiedonsiirto toimii half duplex -periaatteella, eli vain toinen osapuoli, kortti tai lukija, voi lähettää tietoa kerrallaan toisen tällöin kuunnellessa. Myös liikennöintinopeudet ovat samat, 106 kbit/s molempiin suuntiin. (Boussouira 2002, Finkenzeller 2007, OTI Global 2007.)

Lukijasta korttiin päin (downlink) tapahtuva tiedonsiirto perustuu A-standardissa 100 % ASK-modulaatioon. 100 % tarkoittaa, että lukijalaite vaimentaa radiotaajuisen kentän lähes kokonaan tauon luomiseksi, jolloin tehoa ei siirry. A-tyyppi käyttää Miller-koodausta. B-tyypin kortteja käytettäessä lukijalaitteelta korttiin suuntautuva liikenne perustuu RF-kentän 10 % ASK-modulointiin, eli lukijalaite vaimentaa radiotaajuisen kentän vain 10 prosentin verran tauon luomiseksi. Tämän ansiosta sekä kortti että lukija pystyvät ylläpitämään käyttöenergian koko kommunikointiprosessin ajan, mikä on merkittävä etu verrattaessa A-standardin kortteihin. Liikenne lukijasta B-tyypin kortille on koodattu käyttäen NRZ-koodausta, jossa looginen ”1” on sama kuin ei modulointia ja looginen ”0” vastaa 10 % modulointia. (Boussouira 2002, OTI Global 2007.)

Kortilta lukijalle päin (uplink) tapahtuva kuormituksen kommunikaatio perustuu molemmissa standardeissa alikantoaallon modulointiin. Alikantoaallon taajuus on noin 847 kHz ja se syntyy kun kortti kytkee sisäisen kuormansa päälle ja pois, mistä puolestaan seuraa lukijalaitteen generoiman kentän kuormituksen muuttuminen. Alustamisen ja törmäystenhallinnan ajaksi yhden bitin kesto on kahdeksan alikantoaallon jaksoa. Jokainen bitti alkaa määrätyssä suhteessa alikantoaaltoon ja bittijakso alkaa alikantoaallon kuormitustilassa. A-tyypin alikantoaalto on ASK-moduloitua ja data Manchester-koodattua. B-tyyppi käyttää BPSK-modulaatiota (Binary Phase-Shift Keying) ja NRZ-koodausta. (Boussouira 2002, Finkenzeller 2007, OTI Global 2007.)

Lukijalaitteen ollessa tyhjäkäynnillä sen tulee käyttää vuorotellen A- ja B-korttityypin modulointimenetelmiä, kunnes se havaitsee jommankumman korttityypin läsnäolon. Jotta lukijalaite voisi havaita kenttään tulevan kortin, se lähettää toistuvasti pyyntökomentoja (REQuest) odottaen korteilta tulevaa vas-

tausta. Moduloimattomassa kentässä olevan kortin tulee kyetä hyväksymään pyyntö viiden millisekunnin sisällä. Menettelyä kutsutaan pollaukseksi (polling). Jos ATQ-vastaus (Answer To Request) tulee, voidaan olla varmoja, että ainakin yksi kortti on lukuetäisyydellä. Koska lukijan ja tunnisteen välillä tietoa voi samanhetkisesti kulkea vain toiseen suuntaan (half-duplex), lähetyksen suuntaa joudutaan jatkuvasti vaihtelemaan. Molempien standardien korttityypeille on omat pyyntö- ja vastausviestinsä, REQA ja REQB, sekä ATQA ja ATQB. (Boussouira 2002.)

Kortinvalintaprosessin eteneminen on kuvattu kuviossa 27.

KUVIO 27. Lukijan kortinvalintaprosessi (NXP Semiconductors 2006.)

Olipa kyse kummasta korttityypistä tahansa, kortin ja lukijalaitteen välinen alustus käsittää yksinkertaisuudessaan seuraavat toimintovaiheet:

1) Lukijan radiokenttä aktivoi PICC-kortin.
2) Kortti odottaa hiljaisena komentoa lukijalaitteelta.
3) Lukija lähettää komennon.
4) Kortti lähettää vastauksen lukijalle.

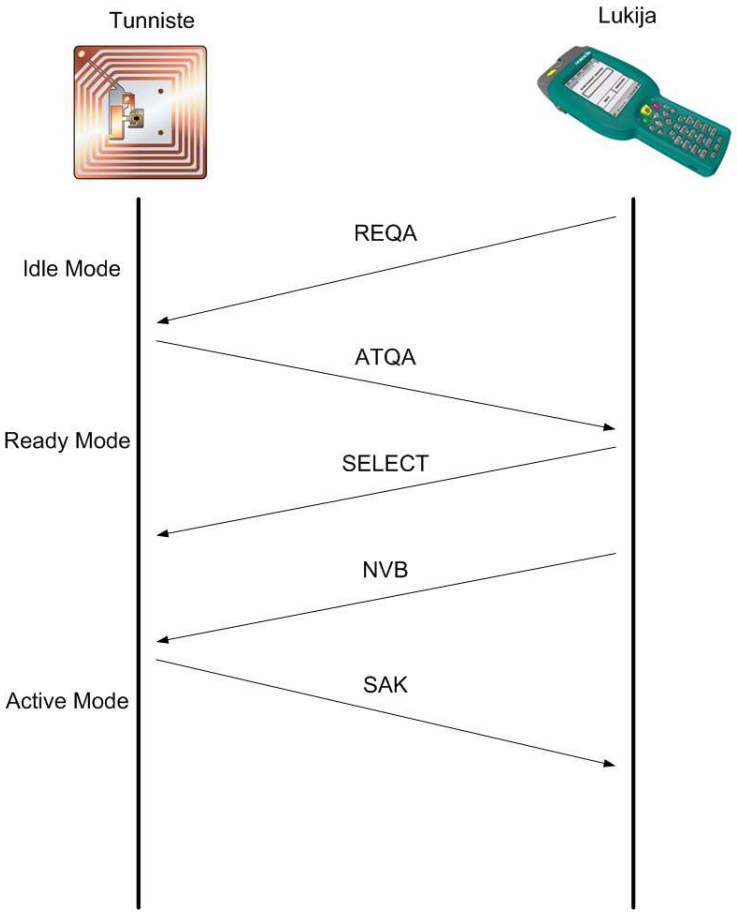
(Koskela 2006.)

TAULUKKO 4. ISO 14443 -standardin A- ja B-tyypit

	A-tyyppi	**B-tyyppi**
Törmäystenhallinta	Search tree -algoritmi	Slotted ALOHA
Downlink (lukija → kortti)		
Modulaatio	ASK 100 %	ASK 10 %
Koodaus	Miller	NRZ
Uplink (lukija ← kortti)		
Modulaatio	ASK (alikantoaalto)	BPSK (alikantoaalto)
Koodaus	Manchester	NRZ

5.4.3 A-tyypin toimintatilat ja tiedonsiirto

Kuviossa 28. on kuvattu A-standardia noudattavan lähilukukortin ja lukijan välinen kommunikointi protokollatasolla. Kortti on oletusarvoisesti odotus- eli idle-tilassa, jossa se on valmis vastaanottamaan lukijan lähettämän Request-pyynnön (REQA). Tätä seuraavat toimenpiteet eroavat A- ja B-standardien korteilla toisistaan. Tunniste vastaanottaa lukijan lähettämän REQA-pyynnön (KUVIO 29.) ja vastaa siihen ATQA-vastauksella (KUVIO 30.) siirtyen samalla odotustilasta (Idle Mode) valmiustilaan (Ready Mode). Kortilta tulleen vastauksen vastaanotettuaan lukija havaitsee kantoalueellaan olevan kortin. (Shepard 2005, 79–81.)



KUVIO 28. Tikapuukaavio A-standardin lähilukukortin ja lukijan välisestä kommunikoinnista.

START	0110	010	END

KUVIO 29. REQA-kehys

START	0-7	Parity	0-7	Parity	0-7	Parity	END

KUVIO 30. ATQA-kehys

Lähilukukorttien A-standardilla törmäystenhallinta perustuu karsintamekanismiin, jonka avulla lukualueella olevien korttien määrä ensin selvitetään ja sit-

ten pikku hiljaa rajataan. Menetelmää kutsutaan muun muassa nimellä Search tree -algoritmi, ja se on esitelty kappaleessa 4.8.
Kun kortinvalintaprosessi törmäyksenhallintoineen on käyty läpi ja on valittu yksi kortti, lukija lähettää valitun kortin sarjanumeron SELECT-komennolla. Kortti vastaa kuittaukseksi SAK-viestillä, joka sisältää myös tiedon kortin tukemasta protokollasta. Mikäli protokolla on ISO 14443 -yhteensopiva, lukija lähettää vielä RATS-komennon (Request for Answer To Select), jonka kortti kuittaa ATS-vastauksella (Answer To Select). Seuraavaksi kortti siirtyy aktiivitilaan (Active Mode), ja varsinainen hyötydatan siirtäminen voi alkaa. (Shepard 2005, 88; 97–98.)

A-tyypin korteilla on seuraavat toimintatilat:

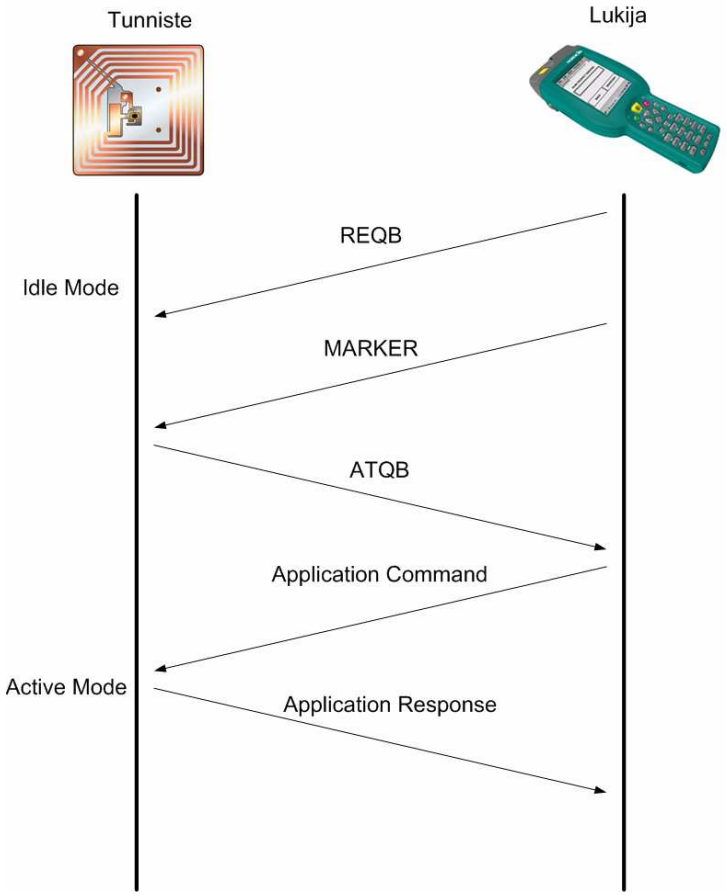
- POWER-OFF: Tässä tilassa kortti ei saa energiaa, eikä pysty toimimaan. Käytännössä se ei siis ole lukijan lukualueella.
- IDLE: Tyhjäkäynti. Kortti saa energiaa ja kykenee demoduloimaan sekä tunnistamaan korttilaitteen lähettämiä REQA- ja WUPA-komentoja.
- READY: Valmiustila. Kortti siirtyy valmiustilaan saatuaan lukijalaitteelta hyväksyttävän REQA- tai WUPA-komennon. Tässä tilassa sovelletaan törmäystenhallintamenettelyä.
- ACTIVE: Aktiivitila. Kortti aktivoituu siirtyen valmiustilasta aktiivitiaan kun se on tullut valituksi omalla tunnisteellaan (UID).
- HALT: Pysähdys. Tila johon kortti siirtyy HALT-komennon tai standardin ulkopuolisen komennon saatuaan. Tässä tilassa kortti vastaa vain WUPA-komentoon, josta se siirtyy READY-tilaan.

(ISO/IEC 1999.)

5.4.4 B-tyypin toimintatilat ja tiedonsiirto

B-standardissa on muutamia erilaisuuksia A:han verrattuna. Protokollatason kommunikointi on kuvattu kuviossa 31. Kun kortti saapuu lukijan lukukentän alueelle, se siirtyy samalla odotustilaan (Idle Mode) odottamaan lukijan Request B -komentoa REQB (KUVIO 32.). B-tyypin järjestelmissä REQB-

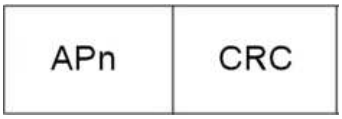
komento aloittaa törmäystenhallintaan liittyvät rutiinit, menetelmä on nimeltään Slotted Aloha (kappale 4.7.4). Menetelmän hallinta on lukijalaitteen vastuulla, sillä lukijalla on tieto törmäysvapaista aikaväleistä (time slot) ja REQB-kehyksessä kortti saa tiedon vapaiden aikavälien määrästä (parametri M, ks. TAULUKKO 5.). Jos määrä on suurempi kuin yksi, kortti arpoo aikaväleistä yhden itselleen ja käyttää sitä lukijalle suunnattuun tiedonsiirtoon. Kortti saa lukijalta vahvistuksen valinnasta MARKER-viestissä (KUVIO 33.). Tämän jälkeen on vielä kortin vuoro vastata Answer to Request B -viestillä (ATQB). (Shepard 2005, 89–91.)



KUVIO 31. Tikapuukaavio B-standardin lähilukukortin ja lukijan välisestä kommunikoinnista

KUVIO 32. REQB-kehys

REQB-kehyksen ensimmäinen kenttä vasemmalta on nimeltään Apf, eli Anti-collision Prefix. Yhden tavun pituinen kenttä kuvastaa kehyksen alkua, ja on bittisisällöltään ”0000 0101”. AFI (Application Family Identifier) sisältää tiedon kyseessä olevasta järjestelmästä tai käyttökohteesta. Esimerkiksi liikenne käyttää AFI-kentässä bittiarvoa ”0001”, maksuihin ja varainsiirtoon käytetään koodia ”0010” ja erilaisille tunnistuskorteille, kuten passeille ja ajokorteille on, varattu koodi ”0011”. Parameter-kenttä voi sisältää järjestelmästä riippuvaa tietoa, kuten vapaiden aikavälien määrän Slotted Aloha -ympäristöissä, tiedon suurimmasta sallitusta kehyskoosta tai tiedonsiirtonopeudesta. Jos kenttää käytetään aikaväleistä tiedottamiseen, siihen sijoitetaan aiemmin mainittu kolmen bitin mittainen M-parametri (TAULUKKO 5.). Viimeinen kenttä, CRC (Cyclic Redundancy Check) on varattu virheenkorjaukselle. (ISO/IEC 1999; Shepard 2005, 89–92.)



KUVIO 33. MARKER-kehys

MARKER-kehyksen avulla lukija välittää kortille tiedot vapaista aikaväleistä. APn-kenttä on yhden tavun mittainen ja muotoa ”nnnn 0101”, jossa ”nnnn” kuvastaa aikavälin numeroa väliltä 1–15. (ISO/IEC 1999.)

TAULUKKO 5. M-parametrin arvot ja vapaat aikavälit (Shepard 2005, 92.)

M-parametri (bitit 0-2)	**Vapaiden aikavälien määrä**
000	1
001	2
010	4
011	8
100	16
101, 110, 111	Varattu myöhempää käyttöä varten.

KUVIO 34. ATQB-kehys

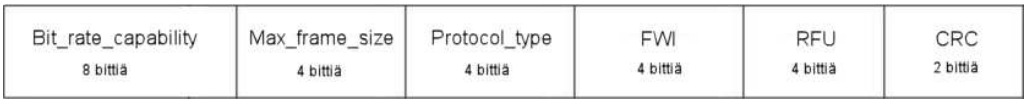
ATQB-kehys (KUVIO 34.) koostuu viidestä kentästä. Ensimmäinen vasemmalta luettuna on yhden tavun mittainen Apa (Anticollision Prefix), joka merkkaa kehyksen alkukohdan. PUPI-kenttä (tavut 2–5) (Pseudo-Unique PICC Identifier) sisältää lähettävän tunnisteen uniikin sarjanumeron. Application Data -kenttä (tavut 6–9) välittää lukijalle tiedon siitä, minkä tyyppistä hyötydataa kortilla on. Tästä voi olla hyötyä kun lukija valitsee useiden kantoalueella olevien korttien joukosta niitä, jotka ovat sen kannalta sillä hetkellä merkittäviä. (ISO/IEC 1999; Shepard 2005, 91–92.)

Protocol Info -kenttä (KUVIO 35.) kattaa tavut 10–12 ja kuljettaa tiedonsiirron kannalta olennaista tietoa kortin ja lukijan välillä. Sen sisältö on jaettu seuraavasti:

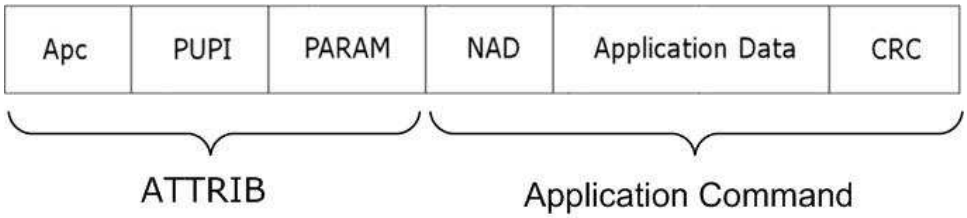
- Bit_rate_capability: Tuetut tiedonsiirtonopeudet. Esimerkiksi bittisarja ”0000 0000” tarkoittaa, että kortti tukee vain 106 kbit/s -nopeuksia molempiin suuntiin.
- Max_frame_size: Suurin mahdollinen kehyskoko.

- Protocol_type: Saa arvon ”0001” jos kortti tukee ISO 14443 -standardia ja kaikilla muilla standardeilla arvon ”0000”.
- FWI (Frame Waiting time Integer): Kehyksen odotusaika.
- RFU (Reserved for Future Use): Varattu tulevaisuuden laajennuksille.
- CRC (Cyclic Redundancy Check): Virheenkorjaukselle varattu tarkistussumma.

(ISO/IEC 1999.)



KUVIO 35. ATQB-kehyksen Protocol Info -kentän sisältö



KUVIO 36. Application Command -kehys

Application Command -kehys (KUVIO 36.) alkaa ATTRIB-etuliitteellä (Attribute), joka sisältää kortin sarjanumeron (PUPI) ja tiedonsiirrossa tarpeellisia tietoja esimerkiksi maksimiviiveistä. Varsinainen Application Command -osuus vastaa ATQB-kehyksen vastaavan kentän sisältöä. (Shepard 2005, 91–92.)

B-tyypin korteilla on seuraavat toimintatilat, jotka eroavat hieman A-tyypin kortin toimintatiloista:

- POWER-OFF: Tässä tilassa kortti ei saa energiaa, eikä pysty toimimaan. Käytännössä se ei siis ole lukijan lukualueella.

- IDLE: Tyhjäkäynti. Kortti saa energiaa ja kykenee demoduloimaan sekä tunnistamaan korttilaitteen lähettämiä REQB- ja WUPB-komentoja.
- READY-REQUESTED: Kortti saa energiaa ja on vastaanottanut hyväksyttävän REQB- tai WUPB-komennon.
- READY-DECLARED: Kortti saa energiaa ja on lähettänyt ATQB-vastauksensa viimeisimmälle hyväksyttävälle REQB- tai WUPB-komennolle.
- ACTIVE: Aktiivitila. Kortti aktivoituu kun se on saanut korttinumeron (CID) hyväksyttävällä ATTRIB-komennolla.
- HALT: Pysähdys. Tila johon kortti siirtyy HALT-komennon tai standardin ulkopuolisen komennon saatuaan. Tässä tilassa kortti vastaa vain WUPB-komentoon, josta se siirtyy IDLE-tilaan. Jos kortti ei saa energiaa, se siirtyy POWER-OFF-tilaan.

(ISO/IEC 1999.)

5.5 Etälukukortit

5.5.1 Yleistä etälukukorteista

Lähilukukorteilla (kappale 5.4) saavutetaan yleensä noin 10 - 25 senttimetrin lukuetäisyydet. Jos korttisovelluksessa tarvitaan tätä suurempia kantomatkoja, seuraava askel on ISO 15693 -standardin mukaiset etälukukortit (VICC), jotka toimivat korkeintaan yhden tai puolentoista metrin etäisyydellä lukijasta. Parempi käyttöetäisyys on saavutettu pääasiassa suuremmalla antennilla. Kortin mitat ovat samat kuin lähilukukorteilla sekä yleisillä pankki- ja luottokorteilla: 3,37 x 2,12 tuumaa, paksuus 0,03 tuumaa. (Shepard 2005, 111–112.)

Tavallisia käyttökohteita ovat yleisötapahtumat, joissa pääsyliput voidaan merkitä RFID-tunnistein. Tekniikkaa käytetään myös lentokentillä matkatavaroiden lajittelussa. Tunnisteen sisältämä yksilöivä koodi on helposti luettavissa ja erotettavissa muista koodeista, minkä lisäksi kortin väärentäminen on hankalaa verrattuna tavanomaisiin paperisiin pääsylippuihin. (Shepard 2005, 111.)

5.5.2 Etälukukortit ja tiedonsiirto

Etälukukortit saavat tiedonsiirrossa tarvitsemansa energian lukijalaitteen (VDC, Vicinity Coupling Device) magneettikentästä, joka toimii 13,56 MHz taajuudella. Magneettikentän voimakkuus on 0,15 – 7,5 A/m. Kortin ja lukijan välinen alustus tapahtuu samoin kuin ISO 14443 -standardissa. Lukijalta kortille päin suuntautuvan tiedonsiirron (downlink) kantoaalto moduloidaan ASK-modulaatiolla, modulaatioindeksinä voi olla lukijalaitteen päätöksen mukaan joko 10 % tai 100 %, kortin on pystyttävä demoduloimaan molemmat. Koodauksessa käytetään kahta erilaista variaatiota PPM-modulaatiosta (Pulse Position Modulation), missä pulssin paikkaa ajansuhteen muutetaan informaatiosignaalin mukaan: 1-of-4 ja 1-of-256. Kortilta lukijaan päin siirtyvä liikenne on koodattu käyttäen Manchester-koodausta, alikantoaalto on ASK- tai FSK-moduloitu. (Koskela 2006, Finkenzeller 2007.)

Tiedonsiirtoprotokollan toiminta perustuu lukijalaitteen tekemään aloitteeseen ja kortin antamaan vastaukseen. Etälukukortilla voi olla neljä tilaa:

- POWER-OFF: Tässä tilassa kortti ei saa energiaa, eli lukija ei pysty aktivoimaan korttia.
- READY: Valmiustila, jossa kortti on sen jälkeen, kun lukija on aktivoinut kortin.
- QUIET: Törmäystenhallintamenettelyn alainen odotustila.
- SELECTED: Kortti vastaa vain pyyntöihin, joissa SELECT-lippu on asetettu. Tämä tila ei ole standardin mukaan pakollinen.

(Koskela 2006.)

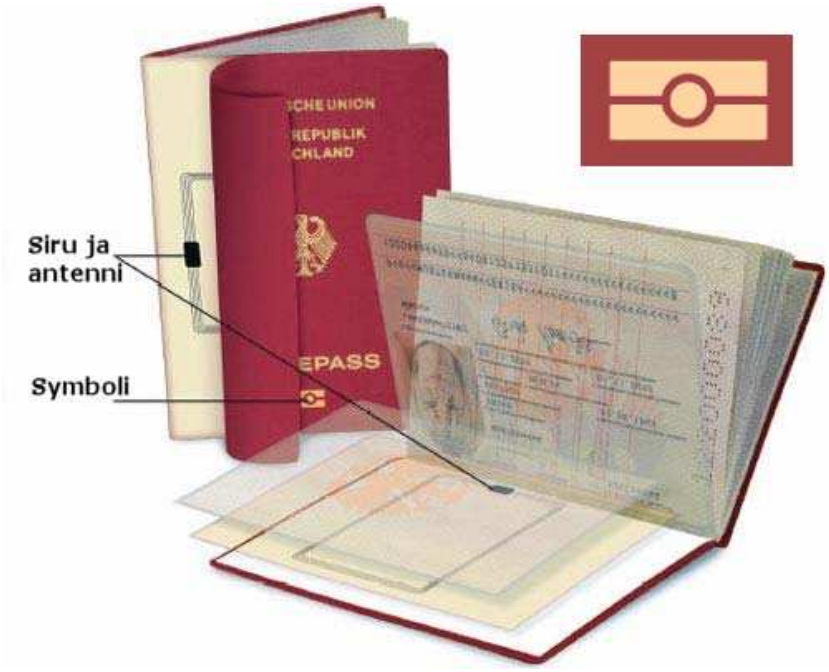
Törmäystenhallinta perustuu lukijan lähettämään INVENTORY-pyyntöön. Kuuluvuusalueella olevat tunnisteet vastaavat lukijalle, ja lukija myöntää lähetysluvan yhdelle kortille kerrallaan. (Koskela 2006.)

6 KÄYTTÖKOHTEITA

6.1 Biopassit

6.1.1 Yleistä biopasseista

Biopassi tai biometrinen passi on passi, jonka sisältämälle RFID-sirulle on tallennettu passin omistajan biologisia tietoja. Tällaisia tietoja voivat olla kasvokuva, silmän iiris tai sormenjälki, joiden lisäksi tallennetaan muun muassa nimikirjoitus sekä perinteiset henkilötiedot kuten nimi, syntymäaika ja kansalaisuus. Biometrinen passi ei ulkonäöltään juuri poikkea perinteisestä passista, paitsi biopasseissa yleensä etukannessa olevan symbolin osalta (KUVIO 37.). (Sisäasiainministeriö 2007.)



KUVIO 37. Biopassi sekä siihen upotetut siru ja antenni (TLfD 2005.)

Tallennettavat tiedot ja muut yksityiskohdat riippuvat noudatettavista asetuksista ja standardeista. Euroopan unionin neuvoston hyväksymän asetuksen mukaan biometrisina tunnisteina käytetään kasvokuvaa ja sormenjälkiä.

Siirtymäaika kasvotunnisteen käyttöönotolle on 18 kuukautta ja sormenjälkien käyttöönotolle 36 kuukautta. Kasvokuvan osalta määräajan laskeminen alkoi 28. päivästä helmikuuta 2005. Käyttöönotto Suomessa tapahtuu kaksivaiheisesti. Ensimmäiset sirulliset passit otettiin käyttöön 21.8.2006, mutta toisen vaiheen ja sen myötä mukaan otettavien sormenjälkien osalta aikataulua ei ole vielä lyöty lukkoon. Suomalaisen biopassin voimassaoloaika on enintään viisi vuotta. (Asetus (EY) N:o 2252/2004; Sisäasiainministeriö 2007.)

Biometristen passien käyttöönottoon päädyttiin, koska rajavalvontaa sekä kansainvälisen terrorismin ja laittoman maahantulon torjuntaa tahdottiin tehostaa. Biometrian avulla valvonta voidaan kohdistaa entistä paremmin, koska voidaan nopeasti tunnistaa ne ihmiset, jotka tulee ottaa tarkempaan tarkasteluun. Biometrisen passin väärentäminen siruineen on huomattavasti perinteistä passia vaikeampaa, minkä lisäksi biometrinen passi vaikeuttaa myös toisen ihmisen täysin aidon passin käyttämistä. (Sisäasiainministeriö 2007.)

6.1.2 Biopassin tekniikka

Biopassin kansainvälisen standardin määrittelee YK:n (Yhdistyneet kansakunnat) alaisuudessa toimiva ICAO (International Civil Aviation Organization). Dokumenteissa passista ja viisumista käytetään nimitystä koneluettavat matkustusasiakirjat, eli MRTD (Machine Readable Travel Document). Biopassin toimintaa määrittelevät lisäksi ISO/IEC 14443 -standardi, josta kerrottiin jo aiemmin kontaktittomien älykorttien kohdalla, sekä ISO 7816 -standardi, joka toimii kaikkien sirukorttien perustana ja johon kaikki muut sirukorttistandardit nojaavat. (ICAO 2007.)

Biopassi sisältää sirun lisäksi antennin. Molemmat on upotettu henkilötietosivun sisään (KUVIO 37.) ja passin kansi toimii suojana, jotta sirua ei pystyttäisi lukemaan kantajan tietämättä. LDS (Logical Data Structure) on passin mikrosirulla oleva tietorakenne, johon passin ja passinhaltijan tiedot on tallennettu. Sirulla on muistia vähintään 32 kilotavua, ja siihen tallennettu kasvokuva on joko JPEG- tai JPEG2000-formaatissa EU-maan oman päätöksen mukaisesti.

JPEG-kuva vie tilaa noin 12–20 kilotavua ja JPEG2000 noin puolet siitä. (Christensen 2007; ICAO 2007; Sisäasiainministeriö 2007.)

Omaa virtalähdettä ei ole, vaan käyttöenergia saadaan lukijalaitteen lähikentästä antennin välityksellä. Säteilyn taajuus on 13,56 MHz ja aallonpituus 22,1 metriä. Passissa käytetään kontaktitonta etäluettavaa sirua, jonka lukeminen ei edellytä sen työntämistä lukijalaitteen sisään. Tämän vuoksi voi syntyä tilanteita, joissa saman lukijan kattamalla lukualueella on useampia kuin yksi passi, jolloin ilman erityisiä törmäyksenestomenetelmiä häiriöiden synty olisi todennäköistä. Myös törmäyksistä ja niiden välttämisestä on kerrottu omassa kappaleessaan älykorttien kohdalla, joita uudet biopassit paljolti muistuttavat. (Christensen 2007; ICAO 2007; Sisäasiainministeriö 2007.)

6.1.3 Biopassien ongelmat ja riskit

Vaikka biopassista pyrittiin tekemään täysin turvallinen ja murtovarma, ei pyrkimyksissä ole täysin onnistuttu. Etäluettavuus tuo helpotusta ja nopeutta passitarkastuksiin, mutta samalla se antaa mahdollisuuden lukea passia etänä myös siellä, missä näin ei ole tarkoitus tehdä. Vaikka standardissa on ilmoitettu lukuetäisyydeksi noin kymmenen senttimetriä, on passia onnistuttu lukemaan jopa kymmenen metrin päästä. Lisäksi Hollannissa on onnistuttu murtamaan biopassin salaus, mikä altistaa passin käyttäjät identiteettivarkauksille.

Hollannissa käytettävän passin salauksen purkamista helpotti huomattavasti passeissa käytetty juokseva numero, jolla oli yhteys passinmyöntämispäivämäärään. Muun muassa Suomen biopasseissa käytetty satunnainen numerointi parantaa kokonaisuuden tietoturvaa. Yhdysvaltalainen Flexilis-yhtiö osoitti kokeessaan vuonna 2006, että Yhdysvalloissa käytetty biopassityyppi pystytään etälukemaan puolen metrin päästä jos passi on hiukankin raollaan. Yhtiö toteutti terroristeja kiinnostavan demon, jossa täsmäpommi asetettiin räjähtämään jos Yhdysvaltojen kansalaisen passi tulee pommin viereen. Yhdysvalloissa passityyppi eroaa toteutukseltaan EU:n biopassista. (Flexilis 2006.)

6.2 NFC – lähialueen langaton yhteystekniikka

6.2.1 Yleistä NFC:stä

Near Field Communication (NFC) on RFID:hen pohjautuva radiotaajuisen etätunnistuksen hyvin lyhyillä etäisyyksillä mahdollistava tekniikka. Suurin käytännön ero RFID:n ja NFC:n välillä on siinä, että RFID-järjestelmässä lukija ja tunniste ovat useimmiten eri laitteita, kun taas NFC-laite toimii samalla sekä lukijana että tunnisteena. NFC on suunnattu pääasiassa kuluttajamarkkinoille, kun taas RFID on fokusoitunut erityisesti teollisuuteen. RFID-taustaisuutensa ansiosta NFC on yhteensopiva lukuisten olemassa olevien kontaktitonta etälukua hyödyntävien palvelujen kanssa. (NFC Forum 2007.)

Kuluttajille suunnattuna tekniikkana NFC:stä on pyritty tekemään mahdollisimman helppokäyttöinen. Tekniikan etuja ovat nopea ja helppo yhteydenmuodostus sekä käyttäjäystävällisyys. Kun kaksi NFC-lähetinvastaanotinta on toistensa kuuluvuusalueella, yhteys niiden välillä on toimintavalmis välittömästi. (Koskela 2006.)

6.2.2 NFC:n toiminnallisuus

NFC ja sen toiminnot on kuvattu standardeissa ISO 18092 sekä ISO 21481. Lisäksi NFC on yhteensopiva ISO 14443 -standardin sekä Philipsin MIFARE- ja Sonyn FeliCa-tekniikoiden kanssa. Yhteys perustuu sähkömagneettikentän induktioon radiotaajuuden ollessa 13,56 MHz. Tiedonsiirtonopeus voi olla 106, 212 tai 424 kbit/s, eli kahden NFC-laitteen välillä voi tyypillisesti siirtää muutamia kilotavuja tietoa. Suurempia tietomääriä käsiteltäessä NFC:tä voi käyttää avaamaan yhteys, jossa varsinainen tiedonsiirto hoidetaan kuitenkin esimerkiksi Bluetoothilla. (NFC Forum 2007.)

NFC-laitteilla on kaksi mahdollista toimintatilaa; passiivinen ja aktiivinen. Kaikkien NFC-laitteiden tulee tukea molempia tiloja.

- Passiivinen toimintatila: Yhteyden alullepaneva laite (initiator) tuottaa radiotaajuuskentän, ja kohdelaite (target) vastaa moduloimalla syntynyttä kenttää. Aloitteentekijä hallitsee tiedonsiirtotapahtumaa. Kohdelaite toimii passiivisesti vastaten saamiinsa pyyntöihin eikä käytä omaa virtalähdettä.
- Aktiivinen toimintatila: Molemmat laitteet kommunikoivat vuorotellen omalla radiotaajuuskentällään. Kun laite odottaa dataa, se sammuttaa oman kenttänsä.

(Koskela 2006.)

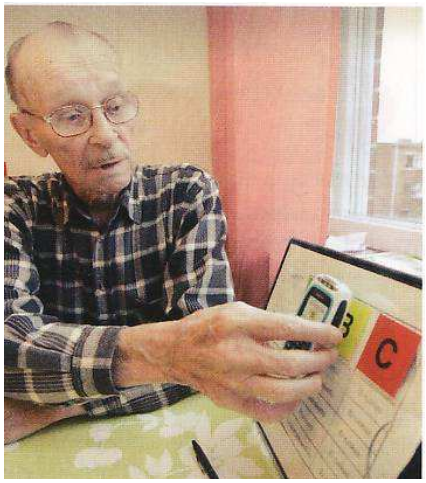
ISO 18092 -standardin laitteet ovat oletuksena kohdelaitteita, eli ne odottavat hiljaisena komentoa aloitteen tekevältä laitteelta. Aloite voidaan saada aikaan laitteeseen asennetun sovelluksen välityksellä. Ohjelmisto myös päättää tiedonsiirtonopeuden sekä sen, toimitaanko passiivisessa vai aktiivisessa kommunikaatiotilassa. Törmäystenhallinta perustuu radiokentän havainnointiin sekä hyvin lyhyisiin lukuetäisyyksiin. Lyhyillä etäisyyksillä törmäysten tapahtumisen todennäköisyys putoaa, mutta niihin on silti varauduttava. Aloitteentekijä testaa ennen radiokentän luontia, onko toista kenttää jo entuudestaan olemassa. Mikäli sellainen havaitaan, ei uutta kenttää muodosteta. Lyhyeen toimintaetäisyyteen liittyy myös tietoturvatekijöitä, sillä muutamien senttimetrin lukuetäisyyksillä salakuuntelun mahdollisuudet vähenevät huomattavasti verrattuna useiden metrien lukuetäisyyksiin. (Koskela 2006.)

6.2.3 NFC käytännössä

NFC:llä on useita merkittäviä tukijoita, joiden avulla se pyrkii valtaamaan sijaa kuluttajien keskuudessa. Yhteistyötä NFC:n kehityksen eteen ovat tehneet muun muassa Mastercard, Microsoft, Nokia, Samsung ja Visa. Nokia julkaisi ensimmäisen NFC:tä tukeneen kännykkämallinsa jo vuonna 2004. Tällaiset puhelimet ovat vielä harvassa, mutta tulevaisuudessa Nokia uskoo tekniikan

yleistyvän voimakkaasti. Sen arvion mukaan vuonna 2010 puolet matkapuhelinmalleista olisi varustettu NFC-sirulla. Koska muun muassa Mastercard ja Visa ovat kiinnostuneet NFC:stä, on hyvin mahdollista, että luottokorttiostokset on tulevaisuudessa mahdollista hoitaa koskettamalla kännykällä kaupan kassalla olevaa NFC-tagia. (Koskela 2006; Vähämaa 2007.)

Yksi NFC:n merkittävistä tulevaisuuden käyttökohteista on erilaisten maksujen, kuten matkalippuostosten hoitaminen. Esimerkiksi bussissa matkustaja voi koskettaa kännykällään NFC-signaalin vastaanottavaa lukijalaitetta, joka rekisteröi signaalin ja matkustaja saa näin matkansa maksettua. Helpoksi käytön tekee myös se, ettei puhelimesta tarvitse etukäteen avata jotain tiettyä sovellusta. Oulussa VTT on testannut vanhusten ruokapalvelussa järjestelmää, jonka piiriin kuuluneet vanhukset ovat voineet kotonaan osoittaa taulusta kännykällä joko A-, B- tai C-kirjainta sen mukaan, mitä ruokaa tahtovat tilata (KUVIO 38.).



KUVIO 38. Ruokatilaus NFC-puhelimella (Vähämaa 2007.)

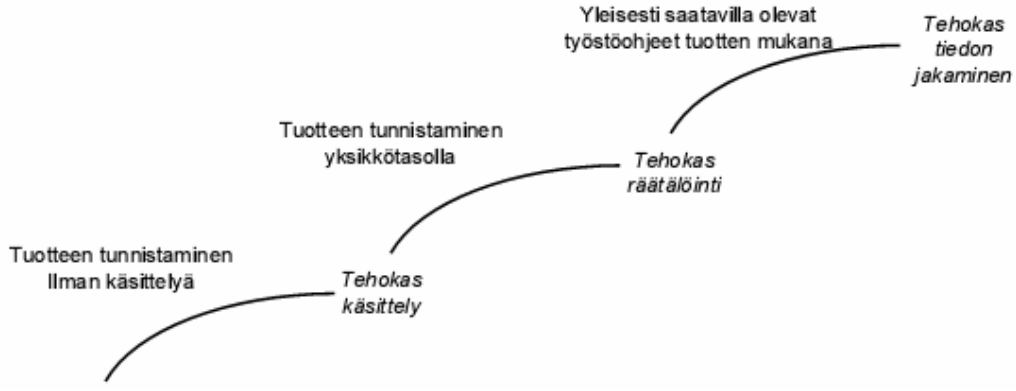
NFC avaa uusia mahdollisuuksia myös mainostajille. Esimerkiksi katumainoksiin tai julisteisiin voidaan upottaa NFC-siru, jota kännykällä koskettamalla saa puhelimen ruudulle lisätietoja tuotteesta tai esimerkiksi ensi-iltaelokuvan videotrailerin. Yksinkertaisimmat NFC-sirut ovat matalan muistikapasiteetin ansiosta hyvin edullisia, mikä nopeuttaa tekniikan yleistymistä. Useimmiten riittää, että siru sisältää viittauksen esimerkiksi www-sivulle, johon matkapuhelin ottaa yhteyden. Suuremmalla muistilla varustettuihin tunnisteisiin voidaan kirjoittaa muutakin informaatiota.

Sonyn kehittämä kontaktiton NFC-älykorttiteknologia on nimeltään FeliCa. Sony ehdotti sitä ISO 14443C -standardiksi, mutta hakemus hylättiin ja nykyi-

sin FeliCa noudattaa NFC:n ISO 18092 -standardia. Tiedonsiirtonopeus on 212 kbit/s ja käytetty taajuus on 13,56 MHz. (Koskela 2006.)

6.3 RFID logistiikassa

Tuotteiden käsittely logistiikkaketjussa tehostuu kun työvaiheet vähenevät ja nopeutuvat RFID:n tarjoaman automaattisen tunnistuksen ansiosta (KUVIO 39.). ABI Research -tutkimusyhtiön mukaan RFID:n käyttö logistiikassa kasvaa nopeammin kuin muilla aloilla. Suurin hyöty RFID:stä logistiikassa saadaan ajoneuvojen, kuljetusyksiköiden, lähetysten ja tavaroiden automaattisesta tunnistamisesta ja kirjautumisesta järjestelmiin normaalissa käsittelyprosessissa. Tunnistamisen yhteydessä lähetys voi kirjautua saman tien esimerkiksi lähetetyksi tai vastaanotetuksi ja ketjun jokaisessa vaiheessa tiedetään tarkkaan missä mikäkin tuote liikkuu. Kun tietoa kerätään varastoihin ja lastauslavoille asetetuilla lukijoilla, sen jälkeen tieto jalostetaan haluttuun muotoon ja jaellaan eteenpäin sitä hyödyntäville osapuolille. Osapuolia ovat esimerkiksi valmistaja, kuljetusyhtiöt, maahantuojat ja jälleenmyyjät. Samalla paranee asiakaspalvelu, koska asiakkaat näkevät reaaliajassa tuotteiden sijainnin logistiikkaketjussa.



KUVIO 39. RFID:llä saavutettavat hyödyt logistiikassa (Kärkkäinen 2004.)

Erityisesti varastoissa ja muissa säilytyspisteissä esineiden automaattinen tunnistaminen tehostaa toimintaa huomattavasti verrattuna vanhoihin viivakoodeihin tai täysin ihmisvoimin toimiviin järjestelmiin. Keskeinen hyödyntämiskohde logistiikassa on häiriötilanteiden hallinta. Seurantatietojen perusteella pyritään mahdollisimman nopeaan häiriöiden tunnistamiseen ja niihin reagoimiseen. Näin korjaavat toimenpiteet voidaan aloittaa riittävän ajoissa esimerkiksi hävikin karsimisessa tai kuljetusten pullonkaulojen korjaamisessa.

6.4 RFID yleisötapahtumissa

RFID nähdään monesti erinomaisena välineenä myös asiakkuudenhallinnassa ja asiakasprofiilien luonnissa. Todennäköisesti aivan lähitulevaisuudessa yleistyvät sovellukset, joissa RFID:tä käytetään erilaisissa yleisötapahtumissa kuten hiihtokeskuksissa ja huvipuistoissa. Jo nykyään lukuisissa huvipuistoissa asiakkaille annetaan ranteeseen kiinnitettävä ranneke merkiksi huvilaitteiden tai muiden palveluiden käyttöoikeudesta. Hyvin suunniteltu RFID-ranneke toisi monta uutta mahdollisuutta ja helpotusta järjestäjälle ja myös asiakkaalle itselleen. Kävijöille pitäisi tarjota myös RFID:tön vaihtoehto. (VTT 2004.)

RFID:n avulla voitaisiin esimerkiksi seurata tarkemmin huvipuiston laitteiden tai hiihtokeskuksen rinteiden käyttömääriä ja kävijöiden profiileja: mitkä ovat suosituimmat laitteet, missä laitteissa kävijät vierailevat, missä järjestyksessä ja mihin aikaan. Ranneke voisi paljastaa perheenjäsenten sijainnin tai vanhemmille kadonneen lapsen olinpaikan. Hiihtäjä voisi olla kiinnostunut hiihtämästään kokonaismatkasta tai jälkikäteen nähtävästä omasta hiihtoreitistä. (VTT 2004.)

6.5 RFID:n tulevaisuus

RFID on viime vuosina tullut vähitellen tunnetuksi erityisesti logistiikassa. Alalla yli 20 vuotta toiminut suomalainen Finn-ID arvioi vuoden 2006 lopulla, että RFID alkaa levitä laajaan käyttöön vuoden 2008 aikana. Se uskoo, että kaupan logistiikkaketjussa käyttö yleistyy seitsemän vuoden kuluessa ja yksit-

täisissä tuotteissa vasta selvästi myöhemmin. Finn-ID:n mukaan viivakoodit ja RFID tulevat olemaan pitkään toisiaan täydentäviä tekniikoita ja niitä käytetään jatkossa sekä erikseen että rinnakkain. Vasta noin vuonna 2013 kauppa alkaa laajemmin hyödyntää RFID:tä tiedonkantajana. (Ojanperä 2006.)

Yhdysvaltain suurin vähittäismyyntiin keskittynyt kauppaketju Wal-Mart on yksi voimakkaimmin RFID:tä tukevista yrityksistä. Vaikka se joutuikin peräänkuulutettuun vaatimuksessaan, jonka mukaan sen yli sadan suurimman tavarantoimittajan olisi pitänyt siirtyä RFID:n käyttöön, Wal-Mart on yhä jatkanut tekniikan puolestapuhujana. Muun muassa merkittävien tukijoiden vuoksi RFID:n kasvu vaikuttaa vakaalta.

Jatkossa tulee yleistymään myös ihmisten merkitseminen tunnisteilla. Esimerkiksi yhdysvaltalainen Applied Digital Solutions valmistaa ihon alle istutettavia VeriChip-siruja (KUVIO 40.), joita on käytetty muun muassa henkilön tunnistamiseen ja tämän terveydentilan tarkkailuun. Tunnisteeseen voidaan tallentaa tiedot henkilöllisyydestä ja muun muassa veriryhmästä, mikä nopeuttaa avunantoa sairaalassa. Siru on pakattu hieman vehnänjyvää suurempaan 11-milliseen ampulliin ja yhtiön mukaan se kestää ihon alle asennettuna noin 20 vuotta. VeriChipin ihonalaista sirua hyödyntää myös Baja Beach Club -yökerho Barcelonassa. Kanta-asiakkaat voivat ottaa kämmenensä ihon alle sirun, ja kättä heilauttamalla drinkit ja sisäänpääsymaksut veloitetaan automaattisesti sirun käyttäjän pankkitililtä. (MBnet 2004, Leidenius 2007.)

KUVIO 40. Ihon alle istutettava RFID-siru (VeriChip 2006.)

Koreassa ollaan suunnittelemassa RFID-tekniikan keskuksiksi kokonaisia kaupunkeja, joista suurimpana New Songdo. New Songdon kuuden neliökilometrin kaupungissa kaikki ihmiset ja esineet merkittäisiin RFID-tageilla. Esimerkiksi pullonpalautusautomaatti tietäisi heti pullon tunnistettuaan, mille pankkitilille hyvitys maksetaan ja yhteiskäyttöisten polkupyörien lainaus suori-

tettaisiin näyttämällä kotiavainta. New Songosta suunnitellaan kaikenlaisen uuden tekniikan testausympäristöä, ja tästä uudesta tekniikasta juuri RFID on merkittävä osa. Kaupunki on arvioitu avattavaksi vuonna 2014. (Leidenius 2007.)

RFID näyttäisi toimivan välivaiheena siirryttäessä niin sanottuihin sensoriverkkoihin, jotka muodostuvat keskenään langattomasti verkottuvista sensoreista. RFID-tekniikassa tieto siirtyy kerrallaan vain kahden pisteen välillä, mutta sensoriverkoissa tieto liikkuu useiden eri sensoreiden välillä ilman erityistä lukemista. Sensorit keskustelevat joko suoraan isäntäkoneen kanssa tai organisoituvat keskenään verkoksi ja vaihtavat tietoja toistensa kanssa. Tekoälyn ansiosta sensorit pystyvät keräämään ympäristöstään tietoa ja käyttöenergiaa itsenäisesti, ja kukin solmu kykenee toimimaan sekä lähettäjänä että vastaanottajana. Tiedonsiirtoon käytetään standardoitua tekniikkaa, kuten Bluetooth, NFC, UWB (Ultra Wideband) tai Zigbee. Sensoreita on jo nyt käytössä teollisuudessa muun muassa maanalaisten rakenteiden kuten vesi- ja sähköverkostojen kunnon seurannassa. Sensorit ovat toistaiseksi vielä kallis ratkaisu, sillä niiden kappalehinta alkaa 15 eurosta. Tutkimusyhtiö Gartnerin ennusteen mukaan hinnat tulevat putoamaan noin 20 prosenttia vuodessa. (Leidenius 2007.)

7 RFID:N TIETOTURVA JA YKSITYISYYS

7.1 Yleistä tietoturvasta

Tietoturvalla tai tietoturvallisuudella tarkoitetaan yleensä tietojen ja tietoliikenteen suojaamista. Tietoturva ja siitä huolehtiminen on tarpeen kaikkialla missä käsitellään tietoa. Tietoturva jaetaan usein kolmeen osa-alueeseen: fyysiseen tietoturvaan, käyttäjien tietoturvaan sekä tekniseen tietoturvaan. Fyysisellä tietoturvalla tarkoitetaan keinoja, joilla suojaudutaan uhkilta fyysisesti, kuten säilyttämällä tiedon tallentamiseen käytettäviä välineitä turvallisissa paikoissa lukituissa tiloissa. Käyttäjien tietoturva on käyttäjiin liittyvien riskien hallintaa esimerkiksi opastuksen ja koulutuksen avulla. Teknisen tietoturvan tavoitteena on, ettei käytetyissä laitteissa ja järjestelmissä ole väärinkäytön mahdollistavia tietoturvapuutteita. (Cibernarium 2005.)

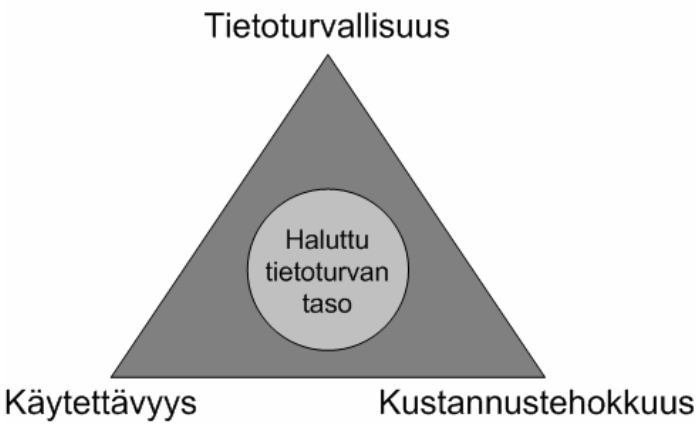
Teknisen tietoturvallisuuden uhkia voivat olla esimerkiksi tietoliikenteen salakuuntelu, erilaiset tietomurrot, huijausyritykset, roskaposti, ohjelmistovirheet sekä virukset ja muut haittaohjelmat. Tekniseen tietoturvaan kuuluu myös laitteiden ja käyttäjien tunnistaminen. Keskenään yhteydessä olevilla tietokoneilla on yleensä omat tunnukset, tunnistetiedot tai jokin muu tapa, jolla ne pystyvät varmistamaan olevansa yhteydessä oikean koneen kanssa. Käyttäjien pääsyä tietojärjestelmiin valvotaan käyttäjätunnusten ja salasanojen avulla. Käyttäjätunnusten, -tasojen ja -ryhmien avulla määritellään mihin tietoihin kullakin käyttäjällä on oikeus päästä käsiksi – joko vain lukemaan tai myös muokkaamaan tietoa. Salasanoihin liittyy aina riskinsä, sillä ne voivat vuotaa ulkopuolisten tietoon joko alkuperäisen omistajan tietämättä tai tarkoituksellisesti. Tietoturvallinen salasana on pitkä ja monimutkainen kirjain- ja numeroyhdistelmä, joka ei sanana tarkoita mitään. Lisäksi salasana kannattaa vaihtaa usein. Teknistä tietoturvaa voi edistää salaamalla tieto tarkoitukseen tehdyllä salausmenetelmällä. Menetelmiä on erilaisia ja eritasoisia, ja valinta niiden välillä riippuu siitä, kuinka vahva salaus halutaan tehdä. (Cibernarium 2005.)

Tietoturva rakentuu kuudesta tekijästä:

- Luottamuksellisuus (confidentiality): Tiedot ja järjestelmät ovat vain niiden käyttöön oikeutettujen tahojen käytettävissä. Kukaan ei siis pääse käyttämään tietoa, jota ei ole hänelle tarkoitettu.
- Eheys (integrity): Tieto ei saa muuttua siirron tai säilyttämisen aikana.
- Käytettävyys (availability): Tiedot ovat aina käyttäjien saavutettavissa tietyn vasteajan puitteissa.
- Pääsynvalvonta (authorization, access control): Käyttäjien pääsyä tietoon rajoitetaan ja valvotaan. Pääsynvalvonnalla tarkistetaan, onko osapuolella oikeus palvelun ja tiedon käyttöön.
- Todennus (authentication): Varmistetaan, että osapuolet ovat niitä, joita sanovat olevansa.
- Kiistämättömyys (non-repudiation): Tiedon todellinen lähettäjä ei voi kiistää lähettäneensä tietoa tai olleensa osallisena jossain tapahtumassa.

(Oulun yliopisto 2007.)

Hyvä tietoturvaratkaisu on yleensä kompromissi tietoturvatason, käytettävyyden ja kustannustehokkuuden kesken (KUVIO 41.). Tietoturvaa rakennettaessa tehokkuuden lisäksi tavoitteena tulee olla yksinkertaisuus, sillä hankalakäyttöinen tietoturvaratkaisu voi muodostua tietoturvauhaksi.



KUVIO 41. Tietoturvallisuuden kolmio

7.2 RFID:n tietoturva

RFID-tunnisteiden luku- ja kirjoitusominaisuudet ovat niiden käytön kannalta olennaisia. Joissain tapauksissa voi olla kuitenkin tarpeen rajoittaa luku- ja kirjoitusoperaatioita siten, että ne ovat vain valtuutettujen lukijalaitteiden tehtävissä. Tageihin on lisätty salasanasuojauksia, mutta puutteellisen laskenta- ja muistikapasiteetin vuoksi suojaukset ovat yleensä heikkoja verrattuna tietotekniikassa yleisimmin käytettyihin suojauksiin. (VTT 2004.)

Kaikkein edullisimmissa tageissa tietoturvaominaisuuksia ei ole lainkaan. Kalliimmat tunnisteet kykenevät esimerkiksi symmetriseen kryptografiaan ja haaste-vaste-autentikointiin. Kaikkein kalleimmissa tunnisteissa on käytetty myös julkisen avaimen kryptografiaa, mutta tällaiset toteutukset ovat ainakin vielä toistaiseksi harvinaisia. (LUOTI 2006.)

Käytännössä kaikki langaton tiedonsiirto on salakuunneltavissa, jolloin tietoturvan tehokkuuden ratkaisee käytettävä salausmenetelmä. RFID:n kohdalla usein luotetaan lyhyen kantaman tuomaan fyysiseen suojaan, sillä salakuuntelu vaikeutuu merkittävästi kun lukuetäisyydet ovat lyhyitä. RFID:llä ei ole yhtenäisiä tietoturvastandardeja, mikä on sekä hyvä että huono asia. Hyvänä puolena on se, että yhden salauksen murtaminen ei tarkoita että samalla periaatteella pystyisi murtamaan seuraavan järjestelmän, mutta toisaalta toteutusten hajanaisuus ja erilaisuus voi häiritä ainakin tekniikan suunnittelu- ja käyttöönottovaiheissa.

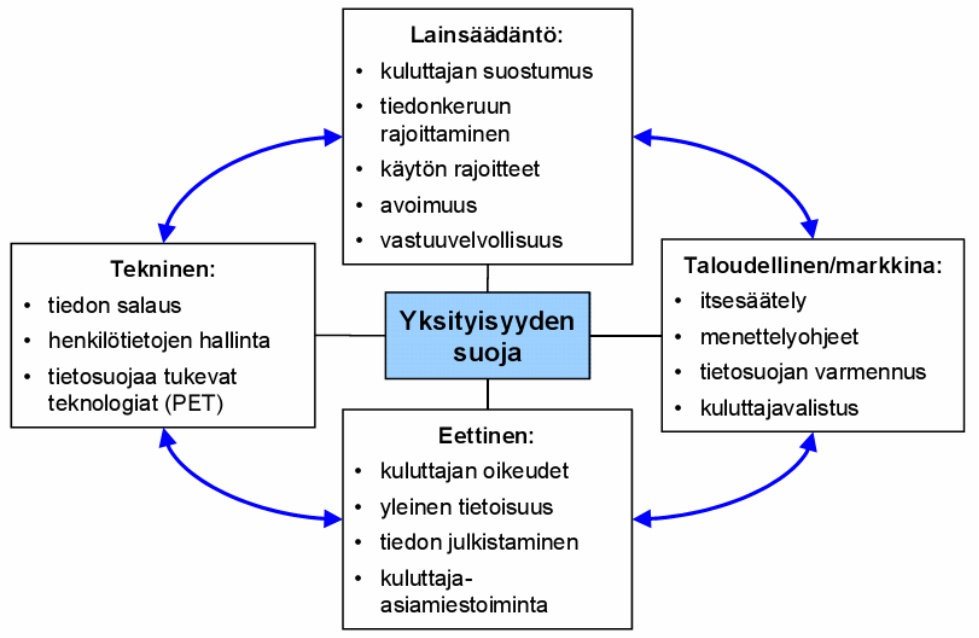
7.3 RFID ja yksityisyyden suoja

Mahdollisuudella lukea tunnisteita langattomasti ja huomaamattomasti on myös kääntöpuolensa. Kun tageja on liitetty ja suunniteltu liitettävän yhä useampiin tuotteisiin ja tavaroihin, on kuluttajajärjestöissä ja kansalaisaktiivien keskuudessa noussut esiin huoli ihmisten yksityisyydensuojasta. Vaikka huolet olisivatkin aiheettomia, on RFID-tekniikkaa hyödyntävien tahojen otettava ne huomioon toteutuksia ja tiedottamista miettiessään. (VTT 2004.)

RFID:n mahdolliset yksityisyyden loukkaamiseen liittyvät ongelmat voivat olla seuraavanlaisia:

- mahdollisuus kerätä salaa tietoa yksityishenkilöistä ja seurata heidän liikkeitään
- mahdollisuus lukea tietoja ihmisten kantamista tuotteista, vaatteista tai esineistä
- kauppojen mahdollisuus luoda tarkennettuja ostajaprofiileja.

Yksityisyyden suojaan liittyy teknisen toteutuksen lisäksi lainsäädännöllisiä sekä asenteellisia ja eettisiä tekijöitä (KUVIO 42.). Lainsäädäntö asettaa omat rajoituksensa henkilötietojen käsittelyyn, minkä lisäksi kuluttajien asenteet uutta teknologiaa ja sen mahdollistamia uhkakuvia kohtaan voivat olla merkittäviä. Muutamat yritykset ovat jo joutuneet luopumaan RFID-teknologian käytöstä kansalaisryhmien painostuksesta, koska tekniikan mahdollistama asiakkaiden seuranta koettiin yksityisyyttä rajoittavana tekijänä. (AINO 2006.)



KUVIO 42. Yksityisyyden suoja eri näkökulmista (AINO 2006.)

Tunnisteissa voi olla niin sanottu KILL-toiminto, jolla tunniste voidaan kytkeä pois päältä, jolloin se ei enää ole jäljitettävissä. Tällaiset toiminnot on tavallisesti piilotettu PIN-koodin, eli staattisen avaimen taakse, jotta kuka tahansa ei pysty käyttämään niitä mihin tahansa tunnisteeseen. Jotkin RFID-tunnisteita tuotteissaan hyödyntävät kaupat ovat hankkineet tiloihinsa erityisiä RFID-tagien deaktivaattoreita, eli laitteita, joilla asiakkaat voivat halutessaan deaktivoida ostamiensa tuotteiden tagit kaupasta lähtiessään. Usein deaktivointi tosin tapahtuu jo kassajärjestelmässä. (LUOTI 2006.)

8 YHTEENVETO

Tämän opinnäytetyön tavoitteena oli tutkia RFID-tekniikkaa ja sen mahdollisuuksia. Aluksi vertailtiin radiotaajuista etätunnistusta sekä perinteistä viivakoodia ja todettiin uuden tekniikan edut, joista suurimpana lukijalaite ei tarvitse näköyhteyttä tunnistettavaan tuotteeseen. RFID-järjestelmästä käytiin läpi oleelliset komponentit ja niiden toiminta sekä tunnistustekniikan mahdollistavat fysikaaliset seikat. Oleellisia asioita ovat muun muassa taajuusalueet ja lähetystehot.

Työssä käytiin lyhyesti läpi myös muissa tietoliikennetekniikoissa oleellisia menetelmiä kuten modulointi, koodaus ja virheenkorjaus. Käyttökohteista perehdyttiin tarkimmin kontaktittomiin älykortteihin, koska niiden tunteminen antaa hyvän kokonaiskäsityksen radiotaajuisesta etätunnistuksesta. Älykortit ovat myös hyvin käytännönläheinen esimerkki aiheesta. Lisäksi tutustuttiin muun muassa biopassiin ja uusiin mahdollisuuksiin logistiikassa, jossa RFID yleistyy kaikkein nopeimmin. Tulevaisuudessa tekniikalla tunnistetaan yhä enemmän myös ihmisiä, ja suunnitteilla on jopa kokonaisia RFID-kaupunkeja.

Lopussa perehdyttiin RFID:n tietoturvaan ja käyttäjien yksityisyyden suojaamiseen. Huolet ovat aiheellisia ja suojaukseen tulee kiinnittää huomiota, sillä langatonta tietoliikennettä voi aina salakuunnella.

Työtä tehdessä nousivat esille tekniikan monikäyttöisyys ja sen luomat mahdollisuudet. RFID on lupaava tunnistustekniikka, joka on jo nyt laajalti käytössä erilaisissa sovelluksissa eri puolilla maailmaa ja uusia toteutuksia julkistetaan jatkuvasti erityisesti teollisuudessa. Kuluttajille suunnatut sovellukset ovat yleistyneet hitaammin. RFID on ollut teknisesti mahdollista jo pitkään. Yhtenäisten standardien puute on kuitenkin ollut merkittävä hidastustekijä sen nopeammalle yleistymiselle. Epäselvyys standardeista luo epätietoisuutta ja hidastaa investointeja uuteen tekniikkaan ja sen käyttöönottoon. RFID on kuitenkin tullut jäädäkseen.

LÄHTEET

Adams, R. 2007. Bar Code History Page [verkkojulkaisu]. Adams Communications [viitattu 3.8.2007]. Saatavissa: http://www.adams1.com/pub/russadam/history.html

AIM 2001. Radio Frequency Identification: RFID [verkkodokumentti]. Automatic Identification Manufacturers [viitattu 15.9.2007]. Saatavissa: http://www.aimglobal.org/technologies/rfid/resources/RFIDPrimer.pdf

AINO 2006. Ajantasaisen liikenneinformaation tutkimus- ja kehittämisohjelma [verkkojulkaisu]. Logistiikan RFID-teknologiakatsaus [viitattu 20.8.2007]. Saatavissa: http://www.ai-no.info/julkaisut/2_kuljinfo/aino_30B_2006_liiteraportti.pdf

Alpha Card 2007. Smart Cards [verkkosivusto]. Saatavissa: http://www.alphacard.com/id-cards/

Asetus (EY) N:o 2252/2004. Annettu Brysselissä 13.12.2004.

Boussouira, R. 2002. Kontaktittomien älykorttien standardin tila ja sisältö [verkkojulkaisu]. Advantec Oy [viitattu 10.7.2007]. Saatavissa: virtual.vtt.fi/fits/julkaisut/hanke1/Raportti_ISO14443_v111.pdf

Cibernarium 2005. Cibernarium-projektin opiskeluaineistosivusto [verkkosivusto]. Saatavissa: http://www.cibernarium.tamk.fi/

EPCglobal 2006. EPCglobal Tag Data Standards Version 1.3 [verkkojulkaisu]. Standardin kuvaus [viitattu 27.10.2007]. Saatavissa: http://www.epcglobalinc.org/standards/tds/tds_1_3-standard-20060308.pdf

Estelle Networks 2006. Definition of RFID [verkkojulkaisu]. Saatavissa: http://www.estellenet.com/rfid.htm

Flexilis 2006. RFID e-Passport Vulnerability [verkkojulkaisu]. Flexilis Inc. [viitattu 15.11.2007]. Saatavissa: http://www.flexilis.com/epassport.php

Finkenzeller, K. 2007. RFID-Handbook [verkkosivusto]. Saatavissa: http://www.rfid-handbook.com

Freeman, M. 1999. Strength in Numbers [verkkojulkaisu]. CRC Theory [viitattu 9.11.2007]. Saatavissa: http://www.netrino.com/Connecting/1999-12/index.php

Goebel, G. 2007. The British Invention of Radar [verkkojulkaisu]. Vectorsite [viitattu 15.6.2007]. Saatavissa: http://www.vectorsite.net/ttwiz_01.html

Granlund, K. 2001. Langaton tiedonsiirto. 1. painos. Jyväskylä: Docendo.

Hämäläinen, P. 2004. RFID tunnistaa kaiken. Tietokone 3/2004.

ICAO 2007. MRTD – Machine Readable Travel Documents [verkkosivusto] [viitattu 16.10.2007]. Saatavissa: http://mrtd.icao.int/content/view/59/228/

ISO/IEC 1999. Final Committee Draft ISO/IEC 14443-3 [verkkojulkaisu]. Saatavissa: http://www.waazaa.org/download/fcd-14443-3.pdf

Jokela, A. 2006. Radiotaajuisen tunnistusteknologian perusteet ja soveltaminen teollisuudessa [luentomateriaali]. Delta-Enterprise [viitattu 12.9.2007]. Saatavissa: http://www.automationit.hut.fi/file.php?id=595

Kalliokoski, S. 2007. RFID – läpinäkyvyyttä logistisiin ketjuihin. RFIDLab. Logistiikan kehittäminen ja uudet työkalut -seminaari.

Korpinen, P. 2005. Heinrich Hertz, sähkömagneettisten aaltojen tutkija [verkkojulkaisu]. Äänipää-verkkojulkaisu [viitattu 12.9.2007]. Saatavissa: http://aanipaa.tamk.fi/hertsi_1.htm

Koskela, M. 2006. Near Field Communication (NFC). Esiselvitys [verkkojulkaisu]. Tampereen teknillinen yliopisto, Porin yksikkö [viitattu 28.10.2007]. Saatavissa: trc.pori.tut.fi/pubdocs/NFC_kitara_mkoskela.pdf

Kuisma, M. 2005a. Modulaatio [luentomateriaali]. Lappeenrannan teknillinen yliopisto.

Kuisma, M. 2005b. EMC ja sähkömagnetismi: Kapasitiivinen, induktiivinen ja RF-kytkeytyminen [luentomateriaali]. Lappeenrannan teknillinen yliopisto [viitattu 21.9.2007]. Saatavissa: http://www.ee.lut.fi/fi/opi/kurssit/Sa2920200/L2-kytkeytyminenweb.pdf

Kärkkäinen, M. 2006. RFID Logistiikassa. Raportti. Saatavissa: http://www.tuta.hut.fi/logistics/publications/RFID_logistiikassa_010806.pdf

Laynetworks 2007. ALOHA Protocol [verkkojulkaisu] [viitattu 15.7.2007]. Saatavissa: http://www.laynetworks.com/ALOHA%20PROTOCOL.htm

Leidenius, K. 2007. Netti kasvaa valvontakoneeksi. Tietokone 11/2007, 22–23.

LUOTI 2006. Luottamus ja tietoturva sähköisissä palveluissa - kehittämisohjelma.

Majander, O. 2004. Tietokone näkee mustaa valkoisella. Mikrobitti 5/2004, 88–90.

MBnet 2004. Jo tuhannelle ihmiselle on istutettu siru [verkkojulkaisu]. Sanoma Magazines Finland Oy [viitattu 21.9.2007]. Saatavissa: http://www.mbnet.fi/uutiset/index.asp?Uutinen=1547

NFC Forum 2007. Verkkosivusto [viitattu 26.10.2007]. Saatavissa: http://www.nfc-forum.org

Nordic ID 2006. Nordic ID PL3000 [kuva]. Saatavissa: http://www.nordicid.com/index.php?m=3&id=98&sm=30

NXP Semiconductors 2006. AN130810 [verkkojulkaisu]. MIFARE ISO/IEC 14443 PICC Selection [viitattu 9.7.2007]. Saatavissa: http://www.nxp.com/acrobat_download/other/identification/M130810.pdf

Ojanperä, V. 2004. RFID kasvaa miljardiluokkaan [verkkojulkaisu]. Prosessori-lehti, Sanoma Magazines Finland Oy [viitattu 17.9.2007]. Saatavissa: http://www.prosessori.fi/uutiset/uutinen.asp?id=45068

Ojanperä, V. 2006. RFID yleistyy vuonna 2008 [verkkojulkaisu]. Tietokone-lehti, Sanoma Magazines Finland Oy [viitattu 13.11.2007]. Saatavissa: http://www.tietokone.fi/uutta/uutinen.asp?news_id=28940

OTI Global 2007. ISO 14443. Saatavissa: http://www.otiglobal.com/objects/ISO%2014443%20WP%204.11.pdf

Oulun yliopisto 2007. Oulun yliopiston tietoturvasivut [verkkosivusto]. Oulun yliopisto [viitattu 7.11.2007]. Saatavissa: http://www.oulu.fi/tietohallinto/tietoturva/

Peltonen, H., Perkkiö, J., Vierinen, K. 2000. Insinöörin (AMK) fysiikka, osa II. 4. painos. Jyväskylä: Gummerus.

Peuhkuri, M. 1996. Lähiverkot [verkkojulkaisu]. Luentomateriaali [viitattu 11.8.2007]. Saatavissa: http://www.netlab.tkk.fi/opetus/s38175/kalvot/960924.shtml

RFID Journal. Genesis of the Versatile RFID Tag [verkkojulkaisu] [viitattu 25.6.2007]. Saatavissa: http://www.rfidjournal.com/article/articleview/392/

RFID Lab Finland 2007. RFID-tietoutta [verkkosivusto] [viitattu 14.11.2007]. Saatavissa: http://www.rfidlab.fi/?1;2;800;800.html

Rintala-Runsala E., Tallgren M. 2004. RFID-tekniikan hyödyntäminen asiakkuudenhallinnassa. TEKES, Tutkimusraportti.

Santanen, M. 2005. RFID-teknologiakatsaus [verkkojulkaisu]. Satakunnan ammattikorkeakoulu [viitattu 19.9.2007]. Saatavissa: http://www.stoy.fi/docs/ub0-RFID_teknologiakatsaus_V1_1AS.pdf

Seppä, H. 2004. Automaattinen tunnistaminen [verkkojulkaisu]. Seminaari [viitattu 21.9.2007]. Saatavissa: http://www.aino.info/seminaarit/syys04/AINO_syys04_Seppa.pdf

Shepard, S. 2005. RFID – Radio Frequency Identification. The McGraw-Hill Companies.

Sisäasiainministeriö 2007. Biometrinen passi [verkkosivusto] [viitattu 16.10.2007]. Saatavissa: http://www.intermin.fi/intermin/hankkeet/biometria/home.nsf/pages/596EE8B62C0D31ABC2256E52002ED3F6

Spurgeon, C. 2001. Ethernet Web Site. Verkkosivusto. Saatavissa: http://www.ethermanage.com/ethernet/ethernet.html

Tamtron Solutions Oy. 2007. RFID-teknologia. Tuote-esite.

Christensen, B. 2007. What is RFID? [verkkosivusto]. Technovelgy.com [viitattu 28.10.2007]. Saatavissa: http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=1

Tekes 2005. Radiotaajuus yhdistää tiedon ja tavarat [verkkojulkaisu]. Saatavissa: http://www.tekes.fi/eu/fin julkaisut/ett/0105/4.html /

TLfD 2005. Landtagskurier 2/2005 [verkkojulkaisu] [viitattu 13.11.2007]. Saatavissa: http://www.thueringen.de/datenschutz/veroeffentlichungen/tlfd/veroeff_landtagskurier/landtagskurier2_05/

ToP Tunniste 2005. Radio Frequency Identification (RFId) kirjastoissa [verkkojulkaisu]. Saatavissa: http://www.kansalliskirjasto.fi/kirjastoala/standardointi/katve/toiminta/Files/liitetiedosto2/TopTunniste.pdf

ToP Tunniste 2006. Identified by ToP Tunniste [verkkosivusto]. Saatavissa: http://www.toptunniste.fi/index.php?id=68

Varpula, T. 2003. UHF – Etätunnistamisen uusi teknologia [verkkojulkaisu]. Luentokalvot [viitattu 7.9.2007]. Saatavissa: http://www.uudenmaanosaamiskeskus.fi/rfid/VTT%20VarpulaRFID%20Mikrotekniikka%202003b.pdf

VeriChip 2006. VeriChip Media Resources [kuva]. Saatavissa: http://www.verichipcorp.com/content/media/resources

VTT 2002. Markku Sipilä: Communications Technologies: The VTT Roadmaps [verkkojulkaisu]. Teknologiakatsaus [viitattu 9.8.2007].Saatavissa: http://www.vtt.fi/inf/pdf/tiedotteet/2002/T2146.pdf

VTT 2004. RFID-tekniikan hyödyntäminen asiakkuudenhallinnassa. Tutkimusraportti.

VTT 2005. Etätunnistusteknologian (RFID) käyttö sähkö- ja elektroniikkalaitteiden kierrätystiedon hallinnassa. Tutkimusraportti.

Vähämaa, M. 2007. Near Field Communication. Uusi Insinööri 1/2007, 40–41.