

TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikan suuntautumisvaihtoehto

Lari Koskinen

RFID-tekniikka ja sen sovellukset

Tutkintotyö, joka on jätetty opinnäytteenä tarkastettavaksi insinööritutkintoa varten
Työn valvoja: Yliopettaja Jorma Punju

Työn nimi:	RFID-tekniikka ja sen sovellukset
Päivämäärä:	18.4.2007
Sivumäärä:	32 sivua
Hakusanat:	RFID
Koulutusohjelma:	Tietotekniikka
Suuntautumisvaihtoehto:	Tietoliikennetekniikka
Työn valvoja:	Yliopettaja Jorma Punju

TIIVISTELMÄ

RFID-tekniikka on yksi nopeasti kehittyvistä tekniikoista, jolle on kaavailtu vankkaa asemaa magneettinauhujen, älykorttien ja viivakoodien syrjäyttäjänä. Viime vuosina RFID-tekniikka on ollut otsikoissa, kun yhdysvaltalainen kauppajättiketju Wal-Mart on siirtynyt käyttämään elektronista tuotekoodia. Myös Nokia on tuonut markkinoille puhelimia, joissa on RFID-lukija. Sen vuoksi on mielenkiintoista perehtyä RFID-tekniikkaan ja sen sovelluksiin.

Työssä tutustutaan hieman RFID-tekniikassa käytettyihin standardeihin ja RFID-tunnisteiden ominaisuuksiin ja niissä käytettyihin komponentteihin. Työssä käydään myös hieman läpi jo käytössä olevia RFID-sovelluksia ja RFID-tekniikan potentiaalisia käyttökohteita. RFID-tekniikan tietoturva on kiperä aihe, joka herättää keskustelua ja siihen on kiinnitetty myös huomiota.

Author: Lari Koskinen
Name of the thesis: RFID technology and its applications
Date: 18.4.2007
Number of pages: 32 pages
Keywords: RFID
Degree programme: Computer Systems Engineering
Specialisation: Telecommunication Engineering

Supervisor: Lecturer Jorma Punju

ABSTRACT

RFID is a one of the swiftly growing technologies which has been planned to play the main role to replace magnetic strips, smart cards and bar codes. Lately RFID technology has been in the headlines when Wal-Mart has moved to use electronic product code. Also Nokia has brought RFID-readers to its mobile phones. There are a lot of interests to use RFID technology. Because of this it is interesting to examine RFID technologies and its applications.

The diploma work go through the standards of RFID, features of RFID tags and components that used in RFID tags. It also present RFID applications, those that are already in use and those potential RFID applications which are intent to use in future. RFID tags' data security is one burning issue and the diploma work intent to look at it.

ALKUSANAT

Tämä insinöörityö on tehty Tampereella keväällä 2007. Valitsin aiheeksi RFID-tekniikan, sillä aihe on hyvin lähellä opinnoissani keskittymiä tietoliikenteen osalueita.

Tampereella 18.4.2007

Lari Koskinen

KÄYTETYT LYHENTEET

ASK	Amplitude-shift keying
CCITT	Comité consultatif international téléphonique et télégraphique
CEPT	European Conference of Postal and Telecommunications Administrations
CMOS	Complementary Metal Oxide Semiconductor
CRC	Cyclic Redundancy check
EEPROM	Electrically Erasable Programmable Read-Only Memory
EAN	European Article Number
EGB	Electromagnetic Band Gap
EPC	Electronic Product Code
ERO	European Radiocommunications Office
ETSI	European Telecommunications Standards Institute
FD	Full Duplex
FSK	Frequency Shift Keying
HD	Half Duplex
HF	High Frequency
ID	Identification
NRZ	Non-Return to Zero
OOK	On-off Keying
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Card
PIFA	Planar Inverted F-antenna
R/O	Read-Only
R/W	Read-Write
RFID	Radio Frequency Identification
TTY	Tampereen Teknillinen Yliopisto
UHF	Ultra High Frequency
UPC	Universal Product Code
VHF	Very High Frequency

VTT	Valtion Teknillinen Tutkimuskeskus
WROM	Write-Once Read Many

SISÄLLYSLUETTELO

TIIVISTELMÄ.....	i
ABSTRACT.....	ii
ALKUSANAT.....	iii
KÄYTETYT LYHENTEET.....	iv
SISÄLLYSLUETTELO.....	vi
1 JOHDANTO.....	1
2 RFID-TEKNIIKAN PERUSTEITA.....	2
2.1 RFID-järjestelmä.....	2
2.2 RFID-tunnisteiden tyypit.....	4
2.3 RFID-tunnisteiden muistit.....	5
2.4 RFID-tekniikan käyttöaajuudet.....	6
2.5 Erilaisten RFID-tunnisteiden ominaisuuksia.....	7
2.6 Esteiden ja metallien vaikutus RFID-järjestelmien toimivuuteen.....	9
2.7 RFID-tunnisteiden standardoinnit.....	9
2.8 RFID-tunnisteissa käytetyt antennit.....	14
3 RFID-JÄRJESTELMIEN SOVELLUKSIA.....	16
3.1 RFID-järjestelmien potentiaalisia käyttökohteita.....	18
4 RFID-JÄRJESTELMIIN LIITTYVIÄ TURVALLISUUSKYSYMYKSIÄ.....	20
5 LOPPUSANAT.....	24
LÄHTEET.....	25

1 JOHDANTO

Tässä työssä tutkitaan RFID-tekniikkaa, siinä käytettäviä komponentteja ja standardeja. Tarkastellaan mm. RFID-tunnisteiden tyyppejä ja niissä käytettyjä muisteja ja antenneja. Esitellään RFID-tekniikassa käytettyjä taajuuksia ja käytössä olevia standardeja. Yleisellä tasolla tarkastellaan myös RFID-tekniikkaan liittyvää tietoturvaa.

RFID-tekniikan sovellukset ovat mielenkiintoinen osa-alue, jossa tarkastell nykyisiä sovelluksia ja tulossa olevia sovelluksia. Jo nyt RFID-tekniikkaa käytetään mm. joukkoliikenteen matkakorteissa, eläinten tunnistuksessa ja passeissa. Tulevaisuudessa olisi houkuttelevaa lisätä RFID-tekniikkaa joka paikkaan, jolloin esineet voitaisiin kytkeä verkkoon. VTT:n tutkijat Nadine Pesonen ja Aarne Oja puhuvat Proessori lehden vuoden 2006 joulukuun numerossa läsnä-älytekniikasta [1]. Automatisointi sensoreiden ja RFID-tekniikan avulla voi olla tulevaisuutta.

2 RFID-TEKNIIKAN PERUSTEITA

RFID (*Radio Frequency Identification*) on automaattinen tunnistusmenetelmä, jossa käytetään RFID-tunnisteita tai transpondereita tiedon tallentamiseen ja lukemiseen radioyhteydellä. RFID-tunniste liitetään tuotteeseen, ihmiseen tai eläimeen tunnistustarkoituksessa. RFID-tunniste luetaan siihen tarkoitettulla lukulaitteella, jolla voi myös tallentaa tunnisteeseen tietoja.

Ensimmäisiä RFID-tunnisteita käytettiin jo toisessa maailmansodassa. Iso-Britannian ilmavoimat käyttivät RFID-tekniikkaa, kun vihollisen lentokone piti tunnistaa omien joukosta. Transponderi tai toisiotutkavastain, joka oli lentokoneessa lähetti lennonjohdon tutkalle koodinsa, josta lentokone voitiin tunnistaa. Transponderi on nykyäänkin käytössä lentokoneissa niin kaupallisella kuin sotilaspuolellakin.

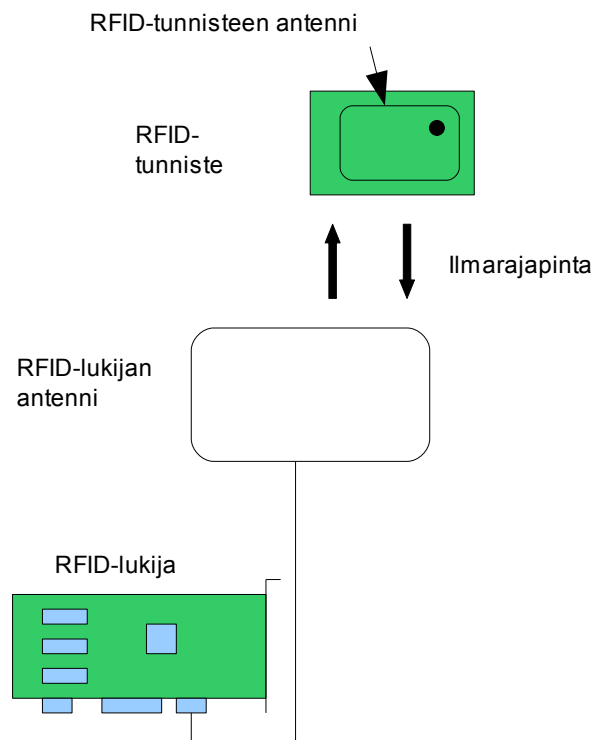
Huomattavaa kehitystä täytyi kuitenkin tapahtua monellakin tieteen osa-alueella, jotta RFID-tekniikkaa voitiin soveltaa entistä enemmän ja paremmin. Piti ratkaista heijastetun käyttöjännitteen siirtoon liittyvät ongelmat.

Vuonna 1973 patentoitiin ensimmäinen moderni takaisinheijastustekniikalla toimiva RFID-tunniste, joka oli passiivinen ja siinä oli muisti.

[2] [3]

2.1 RFID-järjestelmä

RFID-järjestelmään kuuluu RFID-lukulaite, RFID-tunniste ja ehkä muita tiedonkäsittelyjärjestelmiä. Kuvassa 1 on esitetty kaavio RFID-järjestelmästä.



Kuva 1 RFID-järjestelmä kuvattuna

RFID-tunnisteet sisältävät antennin ja mikropiirin. Lisäksi RFID-tunnisteessa voi olla virtalähde tunnisteen tyypin mukaan.

Lukulaitteessa on elektroniikkaa, mikrosiru, muistia ja antenni, joka tulkitsee ja kommunikoi RFID-tunnisteen kanssa. RFID-lukulaitteen prosessori tulkitsee RFID-tunnisteen lähettämän tiedon ja tallentaa sen muistiin. Tiedot voidaan siirtää lukulaitteesta taustajärjestelmään. RFID-tunnisteen lukuetaisyys riippuu sen tehosta, antennista ja taajuudesta.

Yleensä RFID-lukijat voivat lukea yhden RFID-tunnisteen kerrallaan. Jos lukualueella on useampia tunnisteita, niin usein vahvimman signaalin lähettämä RFID-tunniste luetaan. On myös kehitetty protokolla, joka sallii usean RFID-tunnisteen lukemisen yhtä aikaa. Tämä Anti-Collision Protocol eli monilukuprotokolla sallii jopa 100 RFID-tunnisteen yhtäaikaisen lukemisen.

[2] [3] [4]

2.2 RFID-tunnisteiden tyypit

RFID-tunnisteiden tyypit ovat passiivisia, puoliaktiivisia tai aktiivisia.

Passiiviset RFID-tunnisteet

Passiivisessa RFID-tunnisteessa ei ole sisäistä teholähdettä. Sähkövirta indusoituu antenniin radiosignaalista, joka riittää integroidulle CMOS-piirille ja jonka avulla tunniste lähettää vastauksen. Useimmat passiivisten tunnisteiden signaalit toimivat käytännössä sirouttamalla takaisin lukijalaitteen kantoaallon. RFID-tunnisteen antennin täytyy siis pystyä keräämään teho sisään tulevalta signaalilta ja lähettämään signaali ja tämän lisäksi tietoa pitäisi pystyä usein vielä tallentamaan haihtumattomaan muistiin.

Koska passiivinen tunniste ei tarvitse virtalähdettä, voi se olla kokonsa puolesta hyvinkin pieni. Se voidaan sisällyttää esimerkiksi tarraan tai panna ihmisen ihon alle. Esimerkiksi vuonna 2006 Hitachi Ltd. kehitti pienimmän markkinoilla olevan passiivisen tunnisteen, jota se kutsuu nimeltä μ -Chip. Mikrosirun koko ilman antennia on 0,15 mm x 0,15 mm ja paksuutta sillä on vain 7,5 μ m. Mikrosiru voi lähettää oman uniikin 128 -bittisen ID-koodin, jota ei voi muuttaa, mikäli voidaan taata mikrosirun huippulaatuinen todennus. Hitachin μ -Chipin lukuetaisyys on tyypillisesti 30 cm:n säteellä.

Eri yhtiöt kehittelevät myös mikrosiruttomia tai antennittomia RFID-tunnisteita. Kun halutaan poistaa mikrosiru, piin tilalla voidaan käyttää polymeerisiä puolijohteita. Jos polymeerisistä tunnisteista saadaan kehitettyä kaupallisia tuotteita, ovat niiden etuina halvemmat kustannukset verrattuna pii-sirullisiin tunnisteisiin. Myös se, että niitä voitaisiin tulostaa suoraan paperiin luo huikeita näköaloja, sillä näin voitaisiin vaivattomasti ja halvalla korvata viivakoodit. Muita sovelluksia voisi olla mm. pääsylippujen tulostaminen suoraan paperille. Lukuetaisyys siruttomissa RFID-tunnisteissa on kuitenkin yleensä hyvin lyhyt, vain pari senttimetriä.

Aktiiviset RFID-tunnisteet

Aktiivisissa RFID-tunnisteissa on sisäinen virtalähde. Monesti virtalähteenä käytetään litiumparistoa. Aktiiviset tunnisteet ovat luotettavampia kuin passiiviset tunnisteet. Virtalähteen ansiosta aktiivinen RFID-tunniste voi toimia entistä suuremmalla teholla ja näin ollen toimia myös entistä haastavammissa radio-oloissa. Suuren lähetystehon ansiosta sen toimintasäde voi olla satoja metrejä. Aktiivisissa RFID-tunnisteissa on monesti suuremmat muistit kuin passiivisissa RFID-tunnisteissa ja virtalähdekin voi kestää jopa 10 vuotta.

Jotkin aktiiviset RFID-tunnisteet voivat käyttää eri taajuuksia ja näin ollen ne voivat ottaa hyödyn irti sekä pien- että suurtaajuuksien eduista.

Puolipassiiviset RFID-tunnisteet

Puolipassiiviset RFID-tunnisteet ovat aktiivisten ja passiivisten RFID-tunnisteiden sekoitus. Puolipassiivinen RFID-tunniste käyttää omaa virtalähdettä, mutta sillä ei ole omaa lähetystehoja.

[2] [3] [4]

2.3 RFID-tunnisteiden muistit

RFID-tunnisteissa käytetään yksinkertaisimmillaan vain hyvin pieniä muisteja. Kun halutaan tallentaa entistä enemmän tietoja, voidaan käyttää jopa usean kilotavun muisteja.

RFID-tunnisteen muistien tyypit voidaan jakaa kolmeen eri ryhmään, joiden ominaisuuksia ovat muistin lukumahdollisuus, lukumahdollisuus ohjelmoitavuudella tai luku- ja kirjoitusmahdollisuus.

Read-Only-muisteihin (R/O) on tallennettu tuotantovaiheessa oma tunnistuskoodinsa. Read-only-muistia voi ainoastaan lukea. Read-Only -muistin

etuja on sen halpa hinta muihin nähden.

Write-Once Read Many -muistiin (WORM) voidaan yleensä erillisellä laitteella tallentaa uutta tietoa mutta ei RFID-tunnisteen etälukemisen yhteydessä.

Read-Write-muistiin (R/W) voidaan tallentaa tietoa RFID-tunnisteen etälukemisen yhteydessä.

Jos halutaan käyttää tallennusmahdollisuutta passiivisissa RFID-tunnisteissa, käytetään usein EEPROM-muistia (*Electrically Erasable Programmable Read-Only Memory*). EEPROM on haihtumaton puolijohdemuisti, joka ei tarvitse käyttöjännitettä säilyttääkseen dataa.

[2] [4]

2.4 RFID-tekniikan käyttötaajuudet

Periaatteessa jokainen maa määrää taajuudet RFID-laitteille, mutta esimerkiksi Euroopassa on joitakin elimiä (ERO, CEPT ja ETSI), jotka antavat suosituksia taajuuksista ja muistakin aiheeseen liittyvistä standardoinneista.

RFID-tekniikassa on käytössä yleisesti neljä eri taajuusalueetta.

Matalan taajuuden RFID-tunnisteiden toimintataajuus on 125 kHz – 134 kHz ja 140 kHz – 148,5 kHz. Korkean taajuuden tunnisteet toimivat 13,56 MHz:n taajuudella. UHF-tunnisteet toimivat yleensä taajuusalueella 868 MHz – 928 MHz ja mikroaaltotaajuudella toimivat tunnisteet toimivat taajuudella 2,45 GHz tai 5,8 GHz.

Globaalien standardien puute RFID-tekniikassa on edistänyt myös muiden taajuuksien käyttöä. Esimerkiksi taajuusalueella 350 MHz – 433 MHz toimivaa RFID-järjestelmää testataan Englannissa. VHF-taajuudella toimivan järjestelmän etu on pitkä lukuetaisyys, joka on jopa noin 100 metriä ja signaalin hyvä aineiden

läpäisykyky. RFID-järjestelmää testataan Isossa-Britanniassa logistiikan konttien seuranassa ja tulevaisuudessa se olisi tarkoitus lisätä kaikkiin ajoneuvoihin.

RFID-tekniikassa UHF-taajuusalueita ei voi käyttää globaalisti, koska ei ole globaaleja standardeja. Esimerkiksi Yhdysvalloissa voi käyttää lisensioimatonta taajuusalueita 902 MHz – 928 MHz. Euroopassa käytetään yleisesti taajuusalueita 865 MHz – 868 MHz.

[2] [3] [4]

2.5 Erilaisten RFID-tunnisteiden ominaisuuksia

Pien- ja välitaajuudella toimivien RFID-järjestelmien toiminta perustuu magneettikenttiin, kun taas sitä suurempaa taajuutta käyttävien RFID-järjestelmien toiminta perustuu sähkökenttiin.

Taajuudella 125 kHz – 134 kHz toimivia induktiivisia RFID-tunnisteita käytetään, kun ei tarvita pitkää lukuetaisyttä eikä isoa tiedonsiirtonopeutta. Hyväksi ominaisuudeksi voidaan lukea ei-metallisten aineiden mainio läpäisykyky. Huonoksi ominaisuudeksi voidaan laskea monilukumahdollisuuden puute ja hidas tiedonsiirtonopeus. Monesti noin metrin lukualueella toimivia induktiivisia RFID-tunnisteita käytetään mm. henkilöiden kulunvalvontaan, eläinten tunnistukseen ja autojen varkaudenestojärjestelmiin.

Induktiiviset taajuudella 13,56 MHz toimivat ns. älytarrat. Näiden RFID-tunnisteiden lukuetaisyys RFID-lukijalaitteen ominaisuuksien mukaan on 0,6 m – 1,5 m. Ei-metallisten aineiden hyvä läpäisykyky ja kohtuullisen halpa hinta voidaan lukea hyväksi ominaisuuksiksi. Tiedonsiirtonopeus on standardissa enintään 26 kbps, mutta vielä nopeampia lukunopeuksia on ehdotettu standardeiksi. Yleisesti korkean taajuuden RFID-tunnisteita käytetään kirjojen, kuormalavojen, lentolaukkujen ja vaatteiden seurantaan. Korkean taajuuden RFID-tunnisteilla korvataan magneettiraitoja niin henkilöiden kulunvalvonnassa kuin maksukorteissakin.

UHF-taajuudella toimivilla RFID-järjestelmillä voidaan päästä suuriin lukuetaisyyksiin sen mukaan, onko RFID-tunniste passiivinen vai aktiivinen. Taajuusalueella 868 MHz – 928 MHz toimivilla passiivisilla UHF-älytarroilla päästään Yhdysvalloissa 3-4 metrin lukuetaisyyksiin suurimmalla sallitulla 4 watin teholla. Puolet pienemmällä sallitulla teholla päästään Suomessa yli kahden metrin lukuetaisyyteen. Aktiivisilla RFID-tunnisteilla voidaan päästä jopa 100 metrin lukuetaisyyteen. Eräällä järjestelmällä päästään 250 metrin lukuetaisyyteen. Lukualue on yleensä kapea keila. Hyviksi ominaisuuksiksi niin aktiivisille kuin passiivisille suurtaajuudella toimiville RFID-tunnisteilla voidaan lukea moniluvun mahdollisuus ja kohtalainen ei-metallisten aineiden läpäisykyky. Aktiiviset RFID-tunnisteet ovat kalliita, kun taas passiiviset tunnisteet ovat halpoja. UHF-taajuusalueella toimivia RFID-järjestelmiä käytetään yleensä ajoneuvojen tunnistuksissa tai konttien, perävaunujen, kuormalavojen jne. seurannassa rajatulla alueella, kuten satamissa tai varastoalueilla.

Mikroaaltotaajuudella toimivia eli taajuudella 2,45 GHz ja 5,8 GHz sekä vieläkin korkeammalla taajuudella toimivia RFID-järjestelmiä käytetään hieman samoissa paikoissa kuin UHF-taajuudella toimivia RFID-järjestelmiä, kuten esimerkiksi satamissa. Mikroaaltotunnisteiden hyviksi ominaisuuksiksi voidaan lukea nopea tiedonsiirtonopeus ja jopa noin kymmenestä metristä aina 20 metriin ulottuva lukuetaisyys. Huonoiksi ominaisuuksiksi voidaan lukea huono ei-metallisten aineiden läpäisykyky ja usein monilukumahdollisuuden puute. Yleensä mikroaaltotaajuudella toimivat RFID-tunnisteet ovat aktiivisia, mutta on myös kehitetty passiivisia mikroaaltotaajuudella toimivia RFID-tunnisteita.

Monella eri taajuudella toimivia RFID-järjestelmiä on myös kehitetty, ja tällöin RFID-tunnisteessa on eri antennit eri taajuuksille tai ns. monikaista-antenni. Näin voidaan hyödyntää matalien ja suurien taajuuksien tuomia etuja.

[2] [3] [4]

2.6 Esteiden ja metallien vaikutus RFID-järjestelmien toimivuuteen

Metalliset aineet häiritsevät suuresti RFID-järjestelmien käyttöä. Suurilla taajuuksilla antennien toimintataajuus voi muuttua metallien vaikutuksesta ja pienillä taajuuksilla signaali vaimenee. Siksi metallista tehty pinta ei voi toimia RFID-tunnisteen alustana, vaan RFID-tunniste tarvitsee jotain metallisen alustan väliin.

Ei-metalliset aineet eivät aiheuta häiriöitä pientaajuisille RFID-järjestelmille. Mitä suurempaa taajuutta RFID-järjestelmä käyttää, sitä vaikeampaa signaalin on kulkea ei-metallisten esteiden läpi.

[4]

2.7 RFID-tunnisteiden standardoinnit

RFID-järjestelmiä vaivaa globaalien standardien puute. Radiotaajuuksista päättävät Euroopassa CEPT:n (*European Conference of Postal and Telecommunications Administrations*) ja ETSI:n (*European Telecommunications Standards Institute*) kaltaiset järjestöt, joiden taajuus- ja tehostandardeja ja muitakin määräyksiä Suomessa seuraa viestintävirasto. Jokainen maa kuitenkin päättää omista taajuuksistaan. Vaikka Euroopassa olisi standardoitu yhtenäiset taajuusalueet RFID-järjestelmille, niin näin ei ole välttämättä maanosien välillä.

Matalat taajuudet (125 kHz – 134 kHz ja 140 kHz – 148,5 kHz) ja korkea taajuus (13,56 MHz) ovat ainoita taajuuksia, joita voi käyttää globaalisti RFID-järjestelmissä ilman erikoislupia. Muut taajuudet ovat käytössä aluekohtaisesti. Esimerkiksi RFID-järjestelmien UHF-taajuutta ei ole standardisoitu globaalisti, vaan esimerkiksi Yhdysvalloissa käytetään vapaata taajuusaluetta UHF-taajuudella toimiville RFID-järjestelmille, ja samoin Japanissa käytetään eri taajuusaluetta, joka on 952 MHz – 954 MHz. Teho sen sijaan on standardoitu UHF-taajuudella toimiville RFID-laitteille maksimissaan 4 wattiin Yhdysvalloissa, kun se taas Suomessa ja osassa Eurooppaa on 2 wattia. Mikroaaltotaajuudella toimivien

RFID-tunnisteiden taajuus on Euroopassa 2,45 GHz ja 5,8 GHz sekä teho 0,5 wattia, kun taas sisätiloissa säteilyteho saa olla 4 wattia. Standardin ISO 18000 eri osat yrittävät määritellä taajuusalueita ja ilmarajapintoja RFID-järjestelmille, mutta valitettavasti sen osat eivät aina ole täysin yhteensopivia toistensa kanssa.

EPCglobal on maailmanlaajuinen järjestöjen yhteenliittymä, joka on työskennellyt 1990-luvulta lähtien RDIF-tekniikan yhtenäisen standardisoinnin puolesta. Nimensä mukaisesti EPCglobal työskentelee sähköisen tuotekoodin EPC:n (*electronic product code*) globaalien standardisoinnin ja käyttöönoton saralla. EPC Gen2 on sähköisen tuotekoodin standardi ja se on lyhenne sanoista EPCglobal UHF Class 1 Generation 2. EPC Gen 2 omaksuttiin hiljattain pienin muutoksin standardiksi ISO 18000-6C.

Standardien puutteen vuoksi yhtiöt ovat tehneet paljon suljettuja järjestelmiä omilla standardeillaan, jolloin käytössä on erilaisia protokollia ja taajuuksia. Kuitenkin kansainvälisiä standardeja on kehitetty kansainvälisen standardoimiselimien ISO:n toimesta ja tarkastelen seuraavaksi niitä ja niiden tiedonsiirtoprotokollia lyhyesti.

[2] [3] [4]

ISO 11784 ja ISO 11785

ISO 11784/85 on standardi, joka on suunniteltu eläinten tunnistukseen. Standardin mukaan tiedonsiirrossa voidaan käyttää Full Duplex (*FD*) tai Half Duplex (*HD*) -protokollaa. Full Duplex tarkoittaa lähettämistä ja vastaanottamista yhtäaikaaisesti ja Half Duplex tarkoittaa lähettämistä ja vastaanottamista eri aikaan.

Kun on kyse Half Duplex -tiedonsiirrosta, ISO 11784/85 -standardi käyttää taajuusmodulointia (*FSK*). Tällöin taajuus 124,2 kHz tarkoittaa bitin arvoa 1 ja taajuus 134,2 kHz tarkoittaa bitin arvoa 0. Bitin 1 siirtoaika on 0,1288 ms ja bitin 0 siirtoaika on 0,1192 ms. Kokonaisuudessaan yhden datakehysten koko on 112 bittiä. Taulukossa 1 on esitetty datakehysten rakenne.

Taulukko 1 HDX-lähetyksen datakehysten rakenne

Bittien määrä	Bittien paikka	Bittien merkitys
8	1-8	Aloitusbittit
1	9	Eläin/ei eläin
14	10-23	Varattu tulevaan käyttöön
1	24	Data block flag
10	25-34	Maa-koodi
38	35-72	ID-bittit
16	73-88	CRC CCITT -virheenkorjausbittit
24	89-112	Ohjelmabittit

Full Duplex -tiedonsiirrossa ISO 11784/85 -standardi määrittelee modulointitavaksi amplitudimodulaation. Se määrää bitille 1 taajuusalueeksi 129 kHz – 133,2 kHz ja bitille 0 taajuusalueen 135 kHz – 139,4 kHz. Yhden bitin siirtoaika on 0,23845 ms. Half Duplex -protokollassa on helppo napata RFID-tunnisteen heikko signaali, kun RFID-lukijan vahva lähetyssignaali ei ole päällä ja lukija on vain kuunteluasennossa. Protokollan heikkous taas ilmenee siinä, että RFID-tunniste joutuu lähettämään signaalin vain heikkojen kondensaattorien teholla. Taulukossa 2 on esitetty datakehysten rakenne.

Taulukko 2 FDX-lähetyksen datakehysten rakenne

Bittien määrä	Bittien paikka	Bittien merkitys
11	1-11	Aloitusbittit
1	12	Eläin/ei Eläin
14	13-26	Varattu tulevaan käyttöön
1	27	Data block flag
10	28-37	Maa-koodi
38	38-75	ID-bittit
18	76-94	CRC CCITT -virheenkorjausbittit
24	95-118	Ohjelmabittit

Standardi ISO 14223/1 on laajennus standardille ISO 11784/85 ja se yrittää paikata standardin ISO 11784/85 ongelmia. Standardin ISO 11784/85 ongelmat ovat sen puutteet turvallisen ja toimivan eläinten tunnistuksen takaamiseksi. Yksi ongelma on RFID-tunnisteiden valmistajien kyvyttömyys taata yksilöllinen ID-koodi RFID-tunnisteeseen, sillä ei ole kansainvälistä tietopankkia, josta eri valmistajat voisivat tarkistaa sen, että onko ID-koodi jo käytössä. RFID-tunnisteiden avoimeen standardiin perustuva tekniikka ja huono tietoturva antavat mahdollisuuden väärinkäytöksiin. RFID-tunnisteen tietojen muuttaminen ja RFID-tunnisteen kopioiminen on helppoa ja näin ollen kansainvälisten sekä kansallisten lakien ja säädösten huijaaminen ja kierto on mahdollista.

[5] [6] [7]

ISO 14443

RFID-tekniikalla toteutetuissa maksukorteissa ja kulkulupakorteissa voidaan käyttää standardin ISO 14443 mukaista toteutusta, joka toimii taajuusalueella $13,56 \text{ MHz} \pm 7 \text{ kHz}$. Tätä standardia käytetään myös passeissa. Standardi ISO 14443 sisältää useita osia. Standardi nimittää RFID-lukijan lyhenteellä PCD (*proximity coupling device*) ja RFID-tunnisteen lyhenteellä PICC (*proximity integrated circuit card*).

Standardi määrittelee kaksi erilaista protokollatyyppiä, tyyppin A ja tyyppin B. Tyyppin A ja tyyppin B erot liittyvät modulaatiomenetelmiin ja koodaustapoihin.

Tyyppin A kommunikaatiossa PCD-lukijasta PICC-tunnisteeseen käytetään ASK-modulaatiota 100%:n modulaatioindeksillä ja data koodataan Modified Miller-metodilla. Tiedonsiirtonopeus on noin 106 kbit/s.

Tyyppin A kommunikaatiossa PCD-lukijasta PICC-tunnisteeseen käytetään OOK-modulaatiota (*On-Off Keying*) 874,5 kHz alikantoaallolla. Data koodataan Manchester-koodauksella. Tämän protokollan datansiirron ominaisuuksiin kuuluu se, että radiokenttä on aina välillä pois kokonaan, joten PICC-tunniste tarvitsee

tarpeeksi suuret kondensaattorit.

Tyypin B kommunikaatiossa käytetään 10%:n ASK-modulaatiota PCD-lukijasta PICC-tunnisteeseen ja data koodataan NRZ-koodauksella. Kommunikaatiossa PICC-tunnisteesta PCD-lukijaan käytetään BPSK-modulaatiota 847,5 kHz alikantaalla ja data koodataan NRZ-L-koodauksella.

[7] [8] [9]

ISO 15693

Standardi ISO 15693 on myös suosittu tekniikka luottokorteissa ja muissa maksukorteissa. Standardi toimii taajuudella 13,56 MHz ja maksimi lukuetaisyys on pitempi kuin standardissa ISO 14443 eli noin 1 m – 1,5 m.

Standardin ISO 15693 määrittää RFID-lukijaa käyttämään amplitudimodulaatiota (ASK) 10%:n tai 100%:n modulaatioindeksillä ottaessaan yhteyttä RFID-tunnisteeseen. Tällöin käytetään tiedon enkoodaamisessa joko 4-PPM-modulaatiota, jossa jännitetasoja on 4, aikaväli on 9,44 µs ja symboliaika on 75,52 µs, jolloin tiedonsiirtonopeus on 26,48 kbit/s. Toinen vaihtoehto on käyttää 256-PPM-modulaatiota, jossa jännitetasoja on 256, aikaväli on 9,44 µs ja symboliaika on 4,833 ms, jolloin tiedonsiirtonopeus on 1,65 kbit/s [10].

RFID-tunniste lähettää tietoja joko käyttäen hyväksi amplitudimodulaatiota (*ASK*) tai taajuusmodulaatiota (*FSK*).

Amplitudimodulaation modulointi-indeksi on 100% ja apukantaallon taajuus on 423,75 kHz. Datan siirtonopeus voi olla joko 6,62 kbit/s tai 26,48 kbit/s. Looginen nolla ilmaistaan 8 purskeella taajuudella 423,75 kHz, jota seuraa moduloimaton aika 18,88 µs. Looginen ykkönen ilmaistaan toisin päin kuin looginen nolla. Datakehys aloitetaan moduloimattomalla ajalla 56,64 µs, jota seuraa 24 pursketta apukantaalta taajuudella 423,75 kHz ja looginen ykkönen. Datakehys lopetetaan loogisella ykkösellä, jota seuraa 24 pursketta apukantaalta taajuudella 423,75

kHz ja moduloimaton aika 56,64 μ s. Data lähetetään käyttämällä Manchester-koodausta.

Taajuusmodulaatiossa toimitaan taajuuksilla 423,75 kHz ja 484,28 kHz. Tiedonsiirtonopeus voi olla 6,67 kbit/s tai 26,69 kbit/s. Looginen nolla ilmaistaan 8 pursketta taajuudella 423,75 kHz, jota seuraa 9 moduloimatonta pulssia taajuudella 484,28 kHz. Looginen ykkönen ilmaistaan toisin päin kuin looginen nolla. Datakehys aloitetaan 27 purskeella taajuudella 484,28 kHz, jota seuraa 24 pulssia taajuudella 423,75 kHz ja looginen ykkönen. Datakehys lopetetaan loogisella nollalla, jota seuraa taajuudella 423,75 kHz 24 pulssia ja taajuudella 484,28 kHz 27 pulssia. Data lähetetään käyttämällä Manchester-koodausta.

[11] [12]

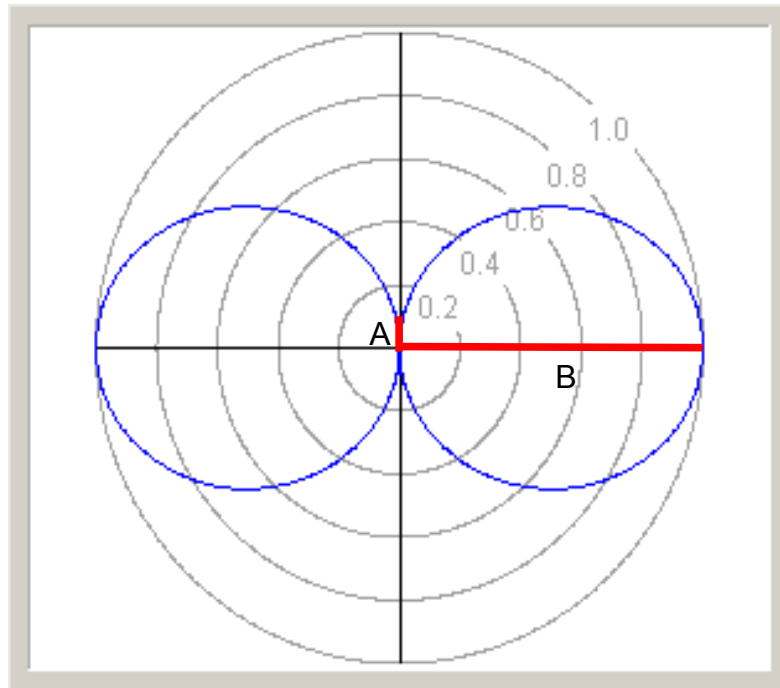
2.8 RFID-tunnisteissa käytetyt antennit

Usein RFID-tekniikassa käytetään muovipohjaista antennitekniikkaa. RFID-tunnisteen taajuudesta riippuvat monesti käytettävän antennin tyypit. HF-taajuudella käytetään usein kela-antenneja, kun taas dipoli-antennit ovat suosittuja UHF-taajuusalueella.

Metallit muuttavat perinteisissä antenneissa viritystä, mutta esimerkiksi VTT on kehittänyt PIFA-antenneja (*Planar Inverted F-antenna*), jotka eivät ole ympäristölle herkkiä. Sovituspiirin käytöltä vältytään, kun antennin impedanssi on sama kuin RFID-tunnisteen syöttöimpedanssi. Eri taajuusalueita taas voidaan yhdistää käyttämällä monikaista-antenneja, jolloin voidaan yhdistää esimerkiksi kela-antenni ja PIFA-antenni. Näin on tehty VTT:n Intellisense RFID -projektissa, jossa on suunniteltu kahta taajuusaluetta käyttävä RFID-tunniste. RFID-tunnistetta voidaan näin ollen lukea HF-taajuudella toimivilla kännykän RFID-lukulaitteella ja UHF-taajuudella toimivalla RFID-lukijalla [1].

Hestnesin vakiota käytetään kuvaamaan RFID-laitteen antennin lukualuetta. Kuvassa 2 on kuvattu Hestnesin vakio, joka lasketaan: antennin etupään

luketäisyys (A) jaettuna sivun luketäisyydellä (B) [2].



Kuva 2 Puoliaaltodipolian antennin säteilykuvio lineaarisella asteikolla

Antennien kokoa yritetään pienentää koko ajan parantamalla EBG-rakenteita (*Electromagnetic Band Gap*). Myös RF-osien sulauttamista antennielementteihin tutkitaan. Tarkoituksena olisi soveltaa uutta tutkimustyötä RFID-lukijoiden antenneihin ja näin ollen pienentää niiden kokoa [15].

Tulevaisuudessa voitaisiin ehkä soveltaa RFID-lukijoissa fraktaaleja antenneja, jotka toimisivat kaikilla taajuusalueilla tai ainakin laajalla taajuusalueella yhtä hyvin. Tämä olisi hyvin kätevää, sillä taajuusalue tilanne RFID-järjestelmissä on maailmanlaajuisesti hyvinkin sekava. Eri taajuusalueita samalla antennilla lukeville RFID-lukijoille voisi olla hyvinkin käyttöä [14].

3 RFID-JÄRJESTELMIEN SOVELLUKSIA

RFID-tunniste passissa

Monissa maissa RFID-tunnisteita on alettu käyttää passeissa. Ensimmäisiä RFID-tunnisteellisia passeja käytettiin Malesiassa 1998. RFID-tunnisteeseen oli tallennettu visuaalinen kuva passin henkilötiedoista ja lisäksi siihen tallennettiin matkahistoria.

Vuoden 2006 alusta Yhdysvalloissa ja Isossa-Britanniassa on otettu uusia RFID-tunnisteisia passeja käyttöön. Passi sisältää omistajan informaation perinteisesti paperilla ja lisäksi samat tiedot digitaalisina passikuva mukaan luettuna. Jotta muut kuin viranomaiset eivät pääsisi lukemaan passin tietoja, on passi suojattu siten, että kun passi on kiinni, niin RFID-tunnistetta suojaa ohut metallivuoraus.

RFID-tunniste maksuvälineenä

Ympäri maailmaa julkisissa kulkuneuvoissa hyödynnetään RFID-tekniikkaa maksuvälineissä. RFID-matkakortti otettiin ensimmäistä kertaa käyttöön Pariisissa vuonna 1995 ja se kuului Calypso-nimiseen maksujärjestelmän standardeihin, ja tämä on sittemmin levinnyt ympäri maailmaan.

Hong Kongissa on samantyyppinen ratkaisu kuin Taiwanissa. RFID-tekniikkaa hyödyntävä kortti on HongKongissa nimeltään Octopus Card ja sitä voi käyttää myös marketeissa ja pikaruokaloissa.

Monilla teillä on jo hyvän aikaa kerätty tiemaksuja RFID-tunnisteita hyväksi käyttäen. Esimerkiksi Norjassa kaikki tiemaksupisteet on varustettu AutoPass-nimisellä RFID-maksusysteemillä.

Taiwanissa käytetään tiemaksuna RFID-teknologiaa hyödyntävää Easy Card -korttia, joka toimii myös muun muassa metroissa, takseissa, parkkipaikoilla ja

busseissa.

Luottokorteissa ja maksukorteissa RFID-tekniikka tekee tuloaan ja esimerkiksi MasterCard on tuonut markkinoille PayPass -maksuvälineen. American Express taas on tuonut markkinoille ExpressPay -luottokortin. Tulevaisuudessa tullaankin käyttämään enemmän luottokortteja, jotka toimivat ilman fyysistä kontaktia.

RFID-tunniste tavarankirjaston seurannassa

RFID-tekniikkaa käytetään mm. kirjaston kirjojen, pallettien ja konttien seurannassa. Myös kulkulupakorteissa ja henkilöllisyyden tunnistus-korteissa on siirrytty käyttämään RFID-tekniikkaa.

RFID-tunniste autoissa

Mikroaaltotaajuudella toimivia RFID-tunnisteita käytetään autojen pääsykontrollointiin, ja ne tunnistavatkin auton jopa yli 100 metrin päästä. Autojen starttia voidaan kontrolloida RFID-tunnisteella siten, että se ei käynnisty ilman RFID-tunnistetta. Toisaalta ovien aukaiseminen ja startti voidaan laittaa kokonaan RFID-tunnistuksen taakse, jolloin auton ovet aukeavat ja auto starttaa siten, että avain ja RFID-tunniste ovat vain kuljettajan taskussa. Michelin on sisällyttänyt auton renkasiin RFID-tunnisteen, jolla voidaan jäljittää renkaat niiden elinkaaren aikana.

RFID-tunniste implantaatissa

Eläimillä on sovellettu jo pitkään ihon alaisia implanteja, jotka sisältävät RFID-tunnisteen. Myös ihmisillä ollaan soveltamassa entistä enemmän RFID-tunnisteisia implanteja. Pari yökerhoa ovat ottaneet käyttöön tämän menetelmän, jolla voidaan autentisoida ihminen luotettavasti. Myös Meksikon oikeusministeriössä on laitettu joillekin työntekijöille ihonalaisia RFID-tunnisteita. Kuvassa 3 on ihonalainen RFID-implantti.



Kuva 3 RFID-implantti

RFID-tunnisteita inventaarisysteemeissä

RFID-tekniikkaa voidaan hyödyntää inventaariossa, jolloin saavutetaan monia etuja. Saadaan mm. tarkka lista tavaroista, jolloin vältetään epätarkkuuksilta, säästytään vähemmällä työmäärällä ja inventaarion tekeminen on helpompaa.

RFID-tunnisteiden luku kännykällä

Nokia on tuonut markkinoille kännykkäkuoria, jotka on varustettu RFID-lukijalla. RFID-lukijat toimivat HF-taajuudella eli taajuudella 13,56 MHz.

[2] [3]

3.1 RFID-järjestelmien potentiaalisia käyttökohteita

EPC eli sähköinen tuotekoodi

Sähköisen tuotekoodin eli EPC:n (*Electronic product code*) pitäisi olla EAN-viivakoodin ja kansainvälisen tuotekoodin UPC (*universal product code*) seuraaja. RFID-tunnisteilla saavutetaan paljon etuja verrattuna viivakoodeihin. Viivakoodit eivät kuitenkaan poistu välttämättä käytöstä kokonaan, sillä ne ovat paljon halvempia RFID-tunnisteisiin verrattuina ja ne voisivat toimia tietolähteenä elektronisen tuotekoodin rinnalla. Tuotteiden seuranta tuotantoketjussa sähköisen tuotekoodin avulla vaatii terabittejä tietoa. Onkin todennäköistä, että tuotteiden jäljitys tapahtuu kuormalavassa olevalla RFID-tunnisteella ja pakkauksissa

käytetään edelleen viivakoodeja.

Yksilöllinen tunnistus RFID-tunnisteiden avulla on ehdoton vaatimus sähköisessä tuotekoodissa. Yksilöllinen tunnistus auttaa yhtiötä taistelemaan varkauksia ja muita tuotteiden häviämistapoja vastaan. Myös viallisten tuotteiden vetäminen markkinoilta olisi tehokkaampaa, kun kyseiset tuotteet voitaisiin jäljittää. Tämä voisi mahdollistaa myös kuluttajien ostoprofiilin seurannan.

On myös maalailtu tulevaisuudennäkymiä myyntipisteettömistä kaupoista, jolloin automaattiset RFID-lukijat hoitaisivat tuotteiden myynnin ja rahastaminen. Tämä idea vaatii kuitenkin vielä paljon kehitystyötä ja RFID-tunnisteiden halventumista.

[2] [3] [16]

Muita ideoita RFID-tunnisteiden käytölle

Terveystieteissä on suunniteltu useita käyttökohteita RFID-tunnisteille. Esimerkiksi RFID-tunnisteiden avulla voitaisiin tunnistaa potilaat ja päästä käsiksi heidän terveystietoihin. Myös ulkomailla voitaisiin päästä käsiksi RFID-tunnisteen sisältämiin potilastietoihin.

Autoilussa voitaisiin hyödyntää sensoreita, jotka käyttäisivät RFID-tekniikkaa. Voitaisiin tarkkailla esimerkiksi tien kuntoa, säättilaa ja vaikka moottorin melutasoa.

Muutenkin antureiden ja sensoreiden liittäminen RFID-tunnisteeseen tulee varmasti entisestään lisääntymään. Kehitystä voi tosin hidastaa se, että elektroniikan ja anturin välistä rajanpintaa ei ole vielä määritelty yleisellä tasolla. RFID-tekniikka yhdistettynä sensoritekniikkaan voitaisiin hyödyntää automaatiota paikoissa, missä sitä ei ole vielä käytössä.

[1] [2] [3]

4 RFID-JÄRJESTELMIIN LIITTYVIÄ TURVALLISUUSKYSYMYKSIÄ

RFID-tekniologian suurimpana turvallisuushuolena on luvaton RFID-tunnisteiden seuranta tai lukeminen. Muiden skannaamiselle alttiit RFID-tunnisteet ovat uhka niin yksityisille henkilöille kuin yhtiöillekin. Elektroniset tuotekoodit voivat olla uhka kuluttajan yksityisyydelle ja toisaalta tietoturvariski yhtiöiden toimitusketjun hallinnoinnille.

Salausmenetelmät

Toisen asteen suojauksessa käytetään salaustekniikkaa estämään RFID-tunnisteen kopioiminen. Monet RFID-tunnisteet käyttävät hyppelykoodia, jolloin tunnistemuuttuu aina skannauksen jälkeen. Hienoimmissa RFID-järjestelmien salauksissa on käytössä haaste-vaste-menetelmä eli Challenge-Response-metodi, jolloin yhteistä salaisuutta ei lähetetä koskaan turvatonta kanavaa pitkin salaamattomana. Sen sijaan RFID-lukija asettaa haasteen RFID-tunnisteelle, joka vastaa lasketulla tuloksella ja sen yksi osatekijä on yhteinen salaisuus eli avain. Tällainen salausprotokolla voi käyttää symmetristä tai epäsymmetristä salaustekniikkaa.

Luotettavaa salausprotokollaa käyttävät RFID-tunnisteet ovat usein paljon kalliimpia ja vaativat enemmän tehoa kuin yksinkertaisemmat salausmenetelmät. Tämän takia monet valmistajat turvautuvat halvempiin ja näin ollen heikomman tietoturvan omaaviin RFID-tunnisteisiin.

Salausmenetelmiä on purettu menestyksellisesti esimerkiksi Isossa-Britanniassa, jolloin passien RFID-tunnisteiden salaus saatiin purettua 48 tunnissa, jättäen miljoonien kansalaisten tiedot alttiiksi tietojen urkinnalle.

Yksityisyysuoja ja RFID-tunnisteet

RFID-tekniologia on aiheuttanut polemiikkaa yksityisyyden suojan puolesta taistelevien kansalaisjärjestöjen puolelta. Villeimmissä uhkakuvissa yritykset ja

jopa valtiot voisivat tarkkailla kansalaisiaan. Hillityimmissäkin uhkakuvissa on tärkeitä näkökulmia, joihin pitää kiinnittää huomiota.

Yhdysvaltalainen kansalaisjärjestö CASPIAN, joka kutsuu RFID-tunnisteita vakoilusiruksi, epäilee viivakoodien korvaamisen RFID-tunnisteilla alentavan yksityisyyden suoja. He ovat huolissaan neljästä isosta ongelmasta, kun puhutaan RFID-tunnisteista tuotteissa ja yksityisyyssuojasta. Ensinnäkin tuotteen ostaja ei välttämättä ole tietoinen tuotteesta olevasta RFID-tunnisteesta tai ei osaa poistaa sitä. RFID-tunniste voidaan lukea kaukaa tuotteesta tuotteen ostajan tietämättä. Jos tuote ostetaan luottokortilla, voitaisiin tuotteesta olevan RFID-tunnisteen yksilöllisen tunnistuskoodin avulla yhdistää tuote ja sen ostajan henkilöllisyys, jolloin yritykset voisivat tehdä kuluttajanprofiilia tehokkaamman markkinoinnin takia ilman yksilön lupaa. Tuotteiden yksilöllinen ID-koodi onkin yksi huolenaihe kansalaisjärjestöissä.

Moni kritiikki kohdistuu siihen tosiasiaan, että RFID-tunnisteen toiminnallisuus säilyy tuotteen ostamisen jälkeenkin, jolloin sitä voidaan käyttää hyväksi ei-toivotulla tavalla. Tällöin esimerkiksi pysäköidyn auton tavaratilasta voitaisiin selvittää, että onko siellä arvokasta tavaraa. Tähän ongelmaan on vastannut Clipped Tag, jota ehdotti IBM:n kaksi suunnittelijaa. Idea oli, että tuotteen maksusuorituksen jälkeen ostaja voi repiä Clipped Tag RFID-tunnisteesta pois osan, jolloin lukumahdollisuus pitkältä etäisyydeltä poistuu ja RFID-tunniste voidaan lukea vain muutaman senttimetrin päästä. Tämä on usein toteutettu niin, että osa antennista poistetaan repimällä. RFID-tunniste toimii tämän jälkeenkin, jolloin sitä voidaan käyttää tuotteen palautuksessa tai reklamaatiossa.

Toinen yksityisyyssuojaan liittyvä kysymys koskee RFID-tekniikassa käytettyä Anti-Collision -protokollaa. Tässä protokollassa RFID-lukija laskee kaikki RFID-tunnisteet, jotka vastaavat sille. Protokollan ominaisuus voi olla sellainen, että kaikki paitsi viimeinen bitti RFID-tunnisteen tunnistuskoodista voidaan päätellä ainoastaan RFID-lukijan lähetteen perusteella. Tällöin RFID-lukijaa voidaan

salakuunnella ja riskiä suurentaa se seikka, että RFID-lukijan lähetysteho on yleensä suuri, jopa 4 wattia, jolloin signaalia voidaan salakuunnella kilometrien päästä. EPC Gen 2 eli ISO 18000-6C standardin protokolla on erilainen, sillä siinä ei lähetetä tunnistuskoodia ja siihen tämä kritiikki ei ulotu.

On tärkeää huomioida, että RFID-lukijan salakuuntelu on mahdollista kilometrien päästä ainoastaan UHF-taajuudella ja sitä suuremmilla taajuuksilla. Matalien taajuuksien, kuten esimerkiksi taajuuden 13,56 MHz teho vähenee radikaalisti jo muutamien metrien päässä lähettäjistä, jolloin salakuuntelijan tarvitsee olla muutamien metrien päässä.

RFID-tunnisteiden tietojen suojaaminen

Yksi käytännöllisimpiä RFID-tunnisteiden lukemisen estämistavoista on estää RFID-tunnistetta saamasta tehoa mistään sulkemalla sen Faradayn häkkiin. Tämä voidaan toteuttaa magneettikenttää hyväksikäyttävillä matalataajuisilla RFID-tunnisteilla koteloidamalla ne magneettisesti ”pehmeillä” ja korkean permittiivisyyden omaavilla aineilla, kuten raudalla tai mu-metallilla. Mitä suurempi taajuus on kyseessä, niin sitä vaikeampi niiden lukeminen on esimerkiksi metallifolion läpi. HF-taajuudella toimivia RFID-tunnisteita on vaikea lukea ohuen metallifolion läpi ja UHF-taajuudella toimivia RFID-tunnisteita on jo erittäin vaikea lukea koteloinnin läpi. Sen sijaan matalataajuisia RFID-tunnisteita on vaikeampi suojata koteloidamalla, vaikkakin se estää useimmat lukuryitykset.

Muita keinoja estää salakuuntelua on jo aiemmin mainittu antennin pienennys, joka mahdollistaa RFID-tunnisteiden lukemisen ainoastaan senttimetrien päästä ja tämä suojaakin tietoja hyvin pitkälle. Myös tehokkaampi salausmenetelmä RFID-tunnisteen autentisoinnissa on yksi tärkeimmistä avuista tietojen suojaamisessa. Brutaalimpi tapa estää tietojen luku on tehdä RFID-tunnisteen tiedot käyttökelvottomaksi lyömällä sirua terävällä esineellä, jolloin muistipiiri hajoaa. Yhtä raaka tapa tuhota RFID-tunniste on laittaa se mikroaaltouuniin, vaikka onnistuminen voi riippua RFID-tunnisteen antennin muodosta ja taajuudesta.

Sivistyneempi tuhoamistapa onnistuu laitteella, jonka nimi on RFID-Zapper. RFID-Zapper lähettää tarpeeksi vahvan sähkökentän, joka aiheuttaa RFID-tunnisteeseen sen verran suuren sähkövirran, että sen piirit tuhoutuvat. Lisäksi RFID-tunniste voidaan tukkia lähettämällä epäaito lähete, jolloin RFID-tunniste ei voi lähettää. Monissa RFID-tunnisteissa on myös funktio, joka ohjelmoi uudelleen laitteen, jolloin tiedot häviävät.

5 LOPPUSANAT

RFID-tekniikkaa on jo paljon käytössä erilaisissa sovelluksissa ja sen tulevaisuus näyttää valoisalta.

Kun RFID-tunnisteeseen lisätään elektronista anturitekniikkaa, voidaan saada langattomasti reaaliajassa tietoja. TTY:n tutkijat tosin ennustavat RFID-tekniikan jäävän vain välivaiheeksi ja tulevaisuuden olevan sensoriverkoissa [17].

Varma on kuitenkin se, että RFID-tekniikkaa tullaan käyttämään entistä enemmän. Tekniikka on jo valmiina ja tutkimustyötä tarvitaan ainoastaan sovelluksien toimivuuden ja turvallisuuden takaamiseksi. Se fakta, että RFID-tunniste on paperinohut tai se voidaan laittaa ihon alle, tekevät RFID-tekniikasta todella houkuttelevan vaihtoehdon. Loppujen lopuksi ainoastaan mielikuvitus on rajana, kun lähdetään miettimään niitä kaikkia sovelluksia, joita saadaan soveltamalla RFID-tekniikkaa.

[1]

Lähteet

- [1] Nadine Pesonen ja Aarne Oja, Esineet alkavat puhua. Prosessori 12/2006, s.55–57
- [2] <http://en.wikipedia.org/wiki/RFID> [viitattu 1.2.2007]
- [3] <http://fi.wikipedia.org/wiki/RFID> [viitattu 1.2.2007]
- [4] <http://virtual.vtt.fi/inf/julkaisut/muut/2002/tasku%2520raportti.pdf>
[viitattu 1.2.2007]
- [5] http://en.wikipedia.org/wiki/ISO_11784_%26_11785 [viitattu 1.3.2007]
- [6] http://www.rfidnews.com/iso_11784short.html [viitattu 1.3.2007]
- [7] <http://163.23.45.9:8080/rueychi/download/rfid/05112309302529391.pdf>
[viitattu 1.3.2007]
- [8] http://en.wikipedia.org/wiki/ISO_14443 [viitattu 1.3.2007]
- [9] http://www.atmel.com/dyn/resources/prod_documents/doc2056.pdf
[viitattu 1.3.2007]
- [10] <http://www.waazaa.org/download/fcd-15693-2.pdf> [viitattu 15.4.2007]
- [11] http://www.aino.info/julkaisut/2_kuljinfo/aino_30B_2006_liiteraportti.pdf
[viitattu 15.3.2007]
- [12] http://en.wikipedia.org/wiki/ISO_15693 [viitattu 1.3.2007]
- [13] http://en.wikipedia.org/wiki/Proximity_card [viitattu 1.3.2007]
- [14] <http://www.tekniikka.info/articles/ST00001.htm> [viitattu 1.3.2007]
- [15] Pasi Raunonen, Mikko Keskilampi, Lauri Sydänheimo ja Markku Kivikoski, Antennien miniatyrisointi. Prosessori 3/2007, s. 46–47
- [16] http://en.wikipedia.org/wiki/Electronic_Product_Code [viitattu 1.3.2007]
- [17] http://www.tietokone.fi/uutta/uutinen.asp?news_id=22165&tyyppi=1
[viitattu 1.3.2007]