LAPPEENRANNAN TEKNILLINEN YLIOPISTO
TIETOTEKNIIKAN OSASTO

RFID-tekniikan käyttö betonielementtien tunnistamiseen

Diplomityön aihe on hyväksytty Tietotekniikan osastoneuvoston kokouksessa 13.12.2006

Työn tarkastajina toimivat Professori Jari Porras ja Dosentti Jouni Ikonen

Lappeenrannassa 22.12.2006

Tommi Kallonen
Snellmaninkatu 13 A 17
53100 Lappeenranta
0500-883770

TIIVISTELMÄ

Lappeenrannan teknillinen yliopisto

Tietotekniikan osasto

Tommi Kallonen

RFID-tekniikan käyttö betonielementtien tunnistamiseen

Diplomityö

2006

64 sivua, 26 kuvaa, 8 taulukkoa

Tarkastajat: Professori Jari Porras ja Dosentti Jouni Ikonen

Hakusanat: RFID, tunnistaminen, betonielementti, langaton tiedonsiirto

Keywords: RFID, identification, concrete-element, wireless communication

RFID on 2000-luvulla yleisesti saatavilla tullut tekniikka erilaisten kohteiden tunnistamiseen. RFID-tekniikassa tunnistamiseen käytetään pienikokoisia tunnisteita, joiden tietosisältö pystytään lukemaan langattomasti ilman näköyhteyttä tarkoitukseen soveltuvalla lukulaitteella. Tunnisteet ovat halpoja ja yksinkertaisia. Yleensä ne eivät sisällä omaa virtalähdettä, vaan ne toimivat ainoastaan lukulaitteen luoman kentän voimalla.

Tässä työssä tutkitaan RFID-tekniikan soveltuvuutta betonista valmistettujen rakennuselementtien tunnistamiseen. Ympäristön vaikutukset tekniikan käyttöön tutkitaan ja selvitetään, mitkä ovat parhaat toimintatavat elementtien tunnistamiseen nämä vaikutukset huomioon ottaen.

Työssä esitellään ensin RFID-tekniikan toimintaperiaatteet sekä tunnisteiden ja lukulaitteiden rakenne. Tunnisteiden jaottelu erilaisten ominasisuuksien perusteella käydään läpi ja sovellusalan kannalta tärkeimmät standardit esitellään. Käytännön osuudessa esitellään RFID-tekniikan soveltamista betonista valmistettujen rakennuselementtien tunnistamiseen. Työssä esitellään saavutetut mittaustulokset sekä betonielementtien tunnistamiseen ja tietojen hallintaan toteutetun järjestelmän rakenne.

ABSTRACT

Lappeenranta University of Technology

Department of Information Technology

Tommi Kallonen

Use of RFID-technology for identification of concrete-elements

Master's Thesis

2006

64 pages, 26 figures, 8 tables

Supervisors: Professor Jari Porras and Adjunct Professor Jouni Ikonen

Keywords: RFID, identification, concrete-element, wireless communication

RFID is relatively new technology for identification of different objects by using simple tags with some memory. Content of the memory can be read from a distance using wireless communication. The tags are simple and inexpensive. Usually they don't have their own power source, so they rely on power achieved from reader's field.

In this thesis the use of RFID-technology for identification of concrete-elements is researched. The affect of concrete elements as an environment with the use of this technology is researched and best practices for the use of RFID-technology in this field are examined.

The beginning of the thesis presents the basics of RFID-technology and the structure of RFID tags and readers. The differentiation of tags by different characteristic is presented and the most important standards for this field are demonstrated. In the practical part of the work the identification of concrete-elements by using RFID tags is tested and results of the measurements are presented. A data system for controlling element and RFID data is implemented and its structure is presented.

LYHENNELUETTELO

CGI	Common Gateway Interface
CRC	Cyclic Redundancy Check
EEPROM	Electrically Erasable Programmable ROM
EPC	Electronic product code
FRAM	Ferroelectric RAM
GID	General Identifier
GPRS	General Packet Radio Service
HF	High Frequency
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
ISO	International Organization for Standardization
LF	Low Frequency
NRZ	Non-Return-to-Zero
PHP	PHP: Hypertext Preprocessor
RAM	Random Access Memory
RFID	Radio Frequency Identification
ROM	Read Only Memory
SQL	Structured Query Language
UHF	Ultra High Frequency
USB	Universal Serial Bus
WWW	World Wide Web

1. JOHDANTO

RFID-tekniikka on ollut suosittu puheenaihe viime vuosina erityisesti logistiikassa. RFID-tekniikassa käytetään pieniä ja edullisia tunnisteita, joiden tietosisältö voidaan etälukea tarkoitukseen soveltuvalla lukulaitteella. RFID-tekniikkaa käytetään usein erilaisten kohteiden tunnistamiseen, sillä RFID-tunniste sisältää yksilöllisen sarjanumeron, jonka avulla kohde voidaan helposti ja luotettavasti yksilöidä. RFID korvaa monin paikoin aikaisemmin käytetyn viivakoodin. Etuja viivakoodiin nähden on useita. Ensinnäkin tunnisteen ja lukulaitteen välillä ei tarvita näköyhteyttä, eli tunniste voi olla piilossa. Toisekseen sopivat tunnisteet kestävät paljon paremmin ympäristöolosuhteita kuin paperiset viivakoodit ja kolmanneksi tunnisteen tietosisältö on paljon suurempi. Viivakoodi kertoo useimmiten ainoastaan tuoteryhmän. RFID-tunnisteita käyttämällä voidaan helposti yksilöidä jokainen tuote.

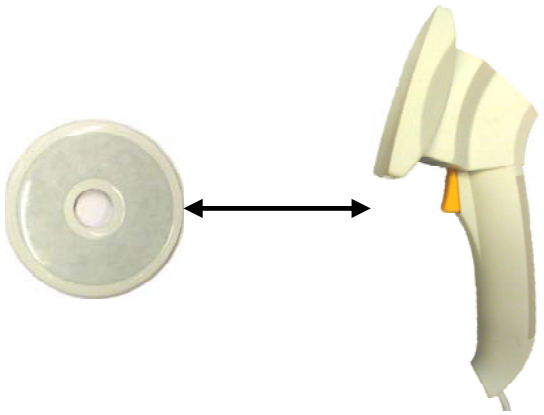
Tässä työssä on selvitetty RFID-tekniikan käyttömahdollisuuksia betonisten rakennuselementtien tunnistamiseen. Rakennuselementtien luotettava yksilöiminen on ollut tähän saakka ongelma. Elementtien tunnistamiseen on käytetty tunnistelappuja sekä viivakoodeja, mutta nämä voivat irrota elementistä jo elementtituotannon aikana tai viimeistään ne irrotetaan rakennusta pystytettäessä. Näin ollen valmiista rakennuksesta yksittäisen elementin tunnistaminen luotettavasti on vaikeaa. Tavoitteena oli selvittää voidaanko elementin sisään upottaa RFID-tunniste, jonka avulla kyseinen elementti voidaan tunnistaa sen valmistamisen ja rakennuksen pystyttämisen aikana sekä valmiissa rakennuksesta ja tunnistamisen jälkeen hakea elementtiin liittyvät tiedot tietokannasta, johon ne on projektin aikana kerätty.

2. RFID – TEKNIIKKA

RFID (Radio Frequency Identification) on ihmisten tai esineiden tunnistamiseen käytettävä tekniikka, joka hyödyntää langatonta tiedonsiirtotekniikkaa. Tunnistettavaan kohteeseen kiinnitetään tunniste, joka voidaan lukea lukulaitteella langattomasti tietyn etäisyyden päästä. Lukuetäisyydet vaihtelevat riippuen käytettävistä tekniikoista ja laitteista muutamista senteistä jopa kymmeneen metriin. Moniin muihin tunnistusjärjestelmiin verrattuna etuna on se, ettei lukulaitteen ja tunnisteen välillä tarvita näköyhteyttä, vaan tunniste voi sijaita jonkin esteen takana tai olla upotettuna kohteeseen. Merkittävä tekijä on myös se, ettei luettava tunniste välttämättä tarvitse omaa virtalähdettä vaan se voi hyödyntää lukulaitteen lähettämää signaalia oman toimintaenergiansa hankkimiseen. Näin ollen tunnisteet voidaan tehdä pieniksi ja ne ovat edullisia. Samalla tunnisteen käyttöikä on todella pitkä, sillä se ei sisällä kuluvia osia. [1]

RFID järjestelmä koostuu siis kahdesta pääosasta, jotka nähdään kuvassa 1:

- Tunniste, joka kiinnitetään tunnistettavaan kohteeseen.
- Lukulaite, jolla luetaan tunnistimen tiedot. Lukulaite voi mahdollisesti myös kirjoittaa piirille tietoa.



Kuva 1. RFID järjestelmän pääosat

Usein lukulaite on kytkettynä tietokoneeseen tai muuhun tietojenkäsittelylaitteeseen. Tällöin tietokone tai muu laite ohjaa lukijan toimintaa syöttäen sille tunnisteelle kirjoitettavat tiedot ja lukemalla siltä tunnisteelta luetut tiedot. Lisäksi järjestelmään kuuluu usein tietojärjestelmä, johon tunnisteista luetut tiedot yhdistetään. Lukulaite huolehtii yleensä tiedonsiirron lisäksi myös virransyötöstä luettavalle piirille. Tässä tapauksessa puhutaan niin sanotuista ”passiivisista tunnisteista”. Lukulaite luo korkeataajuisen magneettikentän, josta luettava piiri saa virtansa antennin avulla. Magneettikentästä indusoituu antenniin jännite, jota luettava piiri

voi käyttää toiminnassaan. Antennina toimivan kelan kanssa rinnan on kytketty kondensaattori. Näiden arvot on valittu niin, että niiden resonanssitaajuus on sama kuin lukulaitteen lähettämän signaalin taajuus. Tunniste voi myös sisältää oman virtalähteen. Tällöin tunniste käyttää omaa virtalähdettä tiedon lähettämiseen. Näillä niin sanotuilla ”aktiivisilla tunnisteilla” saavutetaan yleensä suuremmat lukuetäisyydet kuin passiivisilla tunnisteilla.[1]

Ulkonäöltään tunnisteet voivat olla hyvinkin erilaisia. Osa tunnisteista on tarramallisia ja ne on tarkoitus liimata tunnistettavan kohteen pintaan. Samaan tarraan voidaan myös tulostaa kohteen tiedot ja mahdollisesti viivakoodi, joka toimii vaihtoehtoisena tunnistustapana. Liimattavat tunnisteet ovat edullisia, mutta eivät kovin kestäviä. Mikäli tunnisteelta vaaditaan parempaa fyysistä kestoa, voidaan käyttää muoviin tai lasiin valettuja tunnisteita. Lasitunnisteita käytetään esimerkiksi eläinten tunnistamiseen. Tällöin tunniste sijoitetaan neulan avustuksella eläimen nahan alle. Muovitunnisteita on monen kokoisia ja muotoisia. Ne soveltuvatkin käytettäväksi useissa kohteissa missä liimattavat tarratunnisteet eivät kestä.

Kuva 2. HF taajuusalueella toimiva tarratunnisteita

Kuvassa kaksi nähdään esimerkki HF-taajuusalueella toimivasta kohteen pintaan liimattavasta tunnisteesta. Tunniste on paperipintainen ja se voidaan liimata kohteeseen samalla tavalla kuin muutkin tarrat.

Kuva 3. UHF-taajuusalueen kovapintainen tunniste

Kuvassa kolme on esimerkki UHF-taajuusalueella toimivasta kovapintaisesta tunnisteesta. UHF-taajuusalueen tunnisteet ovat muodoltaan pitkulaisia niiden sisältämän dipolin muotoisen antennin vuoksi.

Kuva 4. Kolme HF-taajuusalueen kovapintaista tunnistetta

Kuvassa neljä nähdään kolme erilaista HF-taajuusaluetta käyttävää kovapintaista tunnistetta. Oikean puoleisesta tunnisteesta nähdään hyvin tunnisteen rakenne. Tunnistetta kiertää kahdeksan kierrosta johdinta jonka muodostama kela toimii tunnisteen antennina. Tämän lisäksi kuvasta voidaan nähdä tunnisteen toiminnasta vastaava mikropiiri. Tunnisteen elektroniikka on pinnoitettu muovilla, joka suojaa sitä ympäristön vaikutuksilta.

2.1 Tunnistetyypit

Tunnisteita voidaan luokitella usealla eri perusteella. Ensinnäkin tunnisteet eroavat virransaantiperiaatteeltaan. Tunnisteet voivat toimia *passiivisesti*, jolloin kaikki niiden käyttämä virta saadaan langattomasti lukijalaitteelta, tai ne voivat toimia *aktiivisesti*, jolloin niiden käyttämä virta saadaan tunnisteen omasta paristosta. Lisäksi tunniste voi olla niin sanottu *semipassiivinen*, jolloin osa sen käyttämästä virrasta saadaan paristosta ja osa lukijalaitteelta.

Toiseksi tunnisteita on toimintamahdollisuuksiltaan erityyppisiä. Yksinkertaisia tunnisteita pystytään vain lukemaan, joidenkin tunnisteiden tietosisältö voidaan kirjoittaa vain kerran ja monimutkaisimpien tunnisteiden tiedot voidaan lukea ja kirjoittaa useaan kertaan.

Tämän lisäksi RFID–järjestelmät käyttävät useita eri taajuusalueita. Matalimmalla Low Frequency (LF) –taajuusalueella toimintataajuus on 125 kHz. Seuraavana taajuusalueena on High Frequency (HF) –alue 13.56 MHz taajuudella. Kolmantena taajuusalueena toimii Ultra High Frequency (UHF) –alue noin 900 MHz taajuudella. UHF–taajuusalueella käytettävä tarkka taajuus vaihtelee eri puolilla maapalloa yhteisten standardien puuttuessa.[2]

2.1.1 Passiivinen tunniste

Virransaannin mukaan jaotelluista tunnisteista passiiviset tunnisteet ovat suosituimpia koska ne ovat yksinkertaisia ja täten halpoja, sekä kestäviä, sillä niissä ei ole paristoa, jonka tyhjeneminen lopettaisi tunnisteen toiminnan. Tunnisteet saavat kaiken tarvitsemansa energian lukulaitteen lähettämästä sähkömagneettisesta kentästä. Tästä syystä tunnisteen lukeminen on hitaampaa kuin aktiivisen tunnisteen, sillä tunnisteen on kerättävä tarpeeksi energiaa toimintansa käynnistämiseen ennen kuin sen kanssa voidaan kommunikoida. Samoin lukuetäisyydet ovat lyhyemmät kuin aktiivisilla tunnisteilla, sillä lukulaitteesta saatavan energian määrä pienenee etäisyyden kasvaessa ja jossain vaiheessa virta ei enää riitä tunnisteen toimintaan.

2.1.2 Aktiiviset tunnisteet

Aktiiviset tunnisteet sisältävät oman virtalähteen eivätkä lukijalaitteen signaalia omassa virransaannissa lainkaan. Koska tunnisteen ei tarvitse saada toiminnassaan tarvittavaa virtaa lukulaitteen signaalista, voi se kommunikoida lukulaitteen kanssa suuremmilla etäisyyksillä kuin passiivinen tunniste[1].

Tunnisteen omaa virtalähdettä voidaan hyödyntää kommunikoinnin lisäksi muuhunkin toimintaan. Tällainen tunniste voi sisältää vaikkapa ympäristöään havainnoivia antureita. Antureista saatava tieto tallennetaan tunnisteen muistiin ja lukulaite lukee tiedot sieltä tunnisteen saavuttua sen läheisyyteen.

Aktiivisten tunnisteiden huonoja puolia ovat hinta sekä pariston kesto. Koska aktiiviset tunnisteen ovat monimutkaisempia kuin passiiviset, on niiden hinta moninkertainen. Aktiivinen tunniste on riippuvainen paristostaan joka tyhjenee ajan kuluessa. Näin ollen aktiivisen tunnisteen käyttöikä ei ole yhtä suuri kuin passiivisen.

2.1.3 Semipassiiviset tunnisteet

Semipassiiviset tai semiaktiiviset tunnisteet sisältävät oman virtalähteen, mutta ne hyödyntävät myös lukulaitteen signaalia virran saantiin. Nämä tunnisteet käyttävät kommunikointiin lukulaitteen signaalia aivan kuten passiivisetkin tunnisteet, mutta käyttävät sen lisäksi omaa virtalähdettä muussa toiminnassaan. Syynä voi olla se, että tunniste havainnoi ympäristöä anturien avulla keräten siitä tietoa [20] tai sitten oman virtalähteen avulla kasvatetaan lukuetäisyyksiä siten että tunniste käyttää lukulaitteen signaalia ainoastaan kommunikointiin, mutta muut toiminnot suoritetaan oman virtalähteen avulla [21]. Tällöin

lukulaitteen signaalista ei tarvitse saada niin paljoa energiaa kuin täysin passiivisen tunnisteen tapauksessa.

2.2 Tunnisteiden ominaisuudet

Tunnisteet voidaan jaotella ominaisuuksiensa mukaan eri luokkiin. Yksinkertaisimmillaan RFID-tunniste ei sisällä mitään tietoa, ainoastaan tunnisteen olemassaolo voidaan havaita. Tunniste voi myös olla vain luettavaa tyyppiä. Tällöin tunniste sisältää ainoastaan sarjanumeron, jota ei voi muokata. Monipuolisempien tunnisteiden tietosisältöä voi myös muokata. Nämä tunnisteet voivat myös sisältää erilaisia tietoturvaominaisuuksia.

2.2.1 1-bittinen piiri

Yksinkertaisin RFID–piiri on niin sanottu 1-bittinen piiri. 1-bittinen piiri ei sisällä varsinaisesti tietoa, kuten sarjanumeroa, vaan ainoastaan sen olemassaolo lukijalaitteen läheisyydessä voidaan havaita. Koska 1-bittinen piiri ei sisällä sarjanumeroa tai muuta tunnistetietoa, ei sitä useinkaan käsitellä RFID-tekniikan osana. 1-bittisen piirin havaitseminen toimii yksinkertaisena esimerkkinä passiivisen piirin ja lukulaitteen välisestä langattomasta kommunikaatiosta, ja näin ollen sen toiminnan ymmärtäminen auttaa ymmärtämään monimutkaisempia RFID-piirejä. Piirin havaitseminen tapahtuu seuraavasti: Lukijalaite luo muuttuvan magneettikentän. Kun luettava tunniste on riittävän lähellä lukulaitetta, sen kelaan indusoituu jännite. Mikäli piirin resonanssitaajuus on sama kuin lukijalaitteen lähettävä taajuus, alkaa se värähdellä. Tämä voidaan huomata lukijalaitteen kelan jännitteen tippumisena.

Lukijalaite ei itse asiassa lähetä vakiotaajuutta, vaan se käy tietyn taajuusalueen läpi alarajasta ylärajaan. Kun muuttuva taajuus osuu samaksi kuin tunnistettavan piirin resonanssitaajuus, tippuu lukijalaitteen kelan impedanssi. Kelan impedanssi on vakio läpi käytävällä taajuusalueella lukuun ottamatta luettavan piirin resonanssitaajuutta. Luettavan piirin olemassaolo havaitaan siis lukijan antennin jännitteen putoamisena luettavan laitteen värähtelytaajuudella.

Koska impedanssin putoaminen on todella pieni, on sen havaitseminen vaikeaa. Luettava piiri voidaankin havaita helpommin seuraavasti: Luettavassa laitteessa on antennin ja kondensaattorin kanssa kytketty vielä rinnan vastus, joka voidaan kytkeä päälle tai pois. Kun tätä vastusta kytketään päälle ja pois tietyllä taajuudella f_s, voidaan tämä havaita lukijalaitteessa. Lukijalaitteen antennin impedanssissa tapahtuu muutokset samalla taajuudella, millä vastusta kytketään päälle ja pois. Tällöin kantoaallon rinnalle muodostuu

alikantoaallot taajuudelle $\pm f_s$. Nämä voidaan suodattaa kaistanpäästösuotimilla ja näin ollen havaita huomattavasti helpommin kuin muutokset antennin jännitteessä lähetystaajuudella. [1]

Samalla periaatteella voidaan lukea myös monimutkaisempaa tietoa sisältäviä piirejä. Mikäli taajuutta f_s ei käytetäkään jatkuvasti, vaan sitä pätkitään, voidaan sen avulla siirtää tietoa luettavasta tunnisteesta lukijalle.

2.2.2 Vain luettavat tunnisteet

Tietoa sisältävistä tunnisteista tämän tyyppiset tunnisteet ovat yksinkertaisimpia ja samalla myös halvimpia vaihtoehtoja. Tunniste sisältää ainoastaan sarjanumeron, jonka perusteella se voidaan tunnistaa. Sarjanumero on talletettu tunnisteen mikropiirille sen valmistusvaiheessa ja tämän jälkeen sitä ei voida enää muuttaa. Kun tällainen tunniste saapuu lukijan läheisyyteen, se alkaa välittömästi lähettää sarjanumeroaan. Tunniste lähettää tätä sarjanumeroa jatkuvasti, niin kauan kuin se vaan on lukijan läheisyydessä.[1]

Tällaiset tunnisteet ovat yksinkertaisuudestaan johtuen todella halpoja valmistaa ja tästä syystä niitä käytetään sovelluksissa, jossa halpa hinta on ensisijaisen tärkeää ja tunnisteen ei tarvitse sisältää muuta tietoa kuin sarjanumero. Useissa sovelluksissa pelkkä sarjanumero riittää, sillä tunnisteeseen liittyvät muut tiedot voidaan tallentaa tietokantaan, josta ne voidaan tarvittaessa hakea.

2.2.3 Luettava/kirjoitettava tunniste

Kirjoitettavia tunnisteita löytyy erikokoisilla muisteilla varustettuina alkaen tavusta useisiin kilotavuihin. Tietojen lukeminen ja kirjoittaminen tapahtuvat useimmiten lohkoissa. Kun lohkon sisältöä halutaan muokata, sen sisältö luetaan ensin lukulaitteen muistiin, siihen tehdään halutut muutokset ja lopulta muokattu lohko lähetetään takaisin tunnisteeseen, jossa se kirjoitetaan muistiin. Nykyjärjestelmissä lohkojen koko vaihtelee kahden ja kuudentoista tavun välillä. Yleensä nämäkin tunnisteet sisältävät normaalin, käyttäjän muokattavissa olevan, muistin lisäksi jo tehtaalla asetetun sarjanumeron, jota käyttäjä ei pääse muokkaamaan, vaan se on ainoastaan luettavissa.[1]

Tällaisia tunnisteita käytetään, kun tunnistettavaan kohteeseen liittyvät tiedot halutaan lukea suoraan tunnisteelta eikä erillisestä tietojärjestelmästä. Erillisen tietojärjestelmän käyttö ei aina ole tarpeellista, ja tallennettaessa tiedot suoraan tunnisteeseen, voidaan järjestelmän rakennetta yksinkertaistaa.

Osa tunnisteista sisältää vielä lisää ominaisuuksia tietojen suojaamiseksi ja tietojen luvattoman lukemisen estämiseksi. Tällaisia tunnisteita käytetään, kun tunnisteet itsessään

sisältävät tietoa jonka muokkaaminen tai päätyminen vääriin käsiin halutaan estää. Ominaisuuksien lisääntyessä myös tunnisteiden hinta kasvaa. Tästä syystä yleensä halutaan käyttää mahdollisimman yksinkertaisia tunnisteita.

2.3 Tiedonsiirto

Tiedon– ja energian siirron ajoittamiseksi passiivisen tunnisteen ja lukulaiteen välillä on kolme eri vaihtoehtoa: half duplex, full duplex ja vuoroittainen tiedonsiirto. Nämä eroavat toisistaan sen mukaan, kuinka tiedon siirtovuorot määräytyvät ja miten tunnisteen tarvitsema energia lähetetään sille.

Half duplex –tilassa tiedonsiirto lukulaitteesta tunnisteeseen tapahtuu eri aikaan kuin tiedonsiirto tunnisteesta lukulaitteeseen. Lukulaite ja tunniste siis vuorottelevat lähetysvuoroja. Lukulaite lähettää kuitenkin kantoaaltoa jatkuvasti, jotta tunniste saa siitä energiansa. Kuvasta 5 nähdään tämä toimintaperiaate. Energian siirto on tauotonta, kun taas tiedonsiirto tapahtuu vuorotellen.

Kuva 5. Tiedonsiirto half duplex periaatteella

Full duplex tilassa toimivassa järjestelmässä tietoa voidaan siirtää sekä lukulaitteelta tunnisteelle, että tunnisteelta lukulaitteeseen yhtä aikaa. Tällöin tiedonsiirto tunnisteelta lukulaitteelle tapahtuu eri taajuudella kuin tiedonsiirto lukulaitteelta tunnisteelle. Tunnisteen lähetystaajuus voi olla jokin lukulaitteen taajuuden kerroin tai täysin itsenäinen taajuus.

Kuva 6. Tiedonsiirto full duplex periaatteella

Vuoroittaista tiedonsiirtoa käytettäessä tiedonsiirto lukulaitteelta tunnisteelle ja tiedonsiirto tunnisteelta lukulaitteelle tapahtuu myös eri aikaan. Tällaisessa järjestelmässä lisäksi energian siirto katkeaa tunnisteen lähettäessä tietoa, eli lukulaite ei lähetä minkäänlaista signaalia tunnisteen lähettäessä tietoa. Tällöin tunniste toimii tietoa lähettäessään varastoimansa energian varassa, ja näin ollen sen on varastoitava riittävästi energiaa lukulaitteen signaalista omaa lähetysvuoroaan varten. Kuvasta 7 nähdään tämän periaatteen mukainen toiminta.

Kuva 7. Vuoroittaisen tiedonsiirron ajoitus

2.4 Käyttöoikeudet

Mikäli kirjoitettavaa tunnistetta ei ole suojattu millään tavalla, mikä tahansa yhteensopiva lukija voi lukea sen tiedot tai kirjoittaa uusia tietoja. Tämä halutaan usein välttää, sillä se voi vaarantaa koko järjestelmän toimivuuden. Esimerkkinä voisi olla julkisen liikenteen maksukortit tai ajonestojärjestelmät. Lisäksi tunnisteiden lukeminen voi olla ongelma yksityisyyden suojan kannalta. Tunnisteita lukemalla voi saada selville esimerkiksi ihmisten tekemät ostokset ja näin vakoilla heidän käyttäytymistään.

Tästä syystä RFID–tunnisteisiin on kehitetty suojajärjestelmiä, jotka estävät asiattomat luku– ja kirjoitustapahtumat. Periaatteena näissä järjestelmissä on se, että ennen kuin tunniste lähettää lukulaitteelle mitään tietoa itsestään, se tarkistaa, onko lukulaitteella oikeus näiden tietojen saamiseen. Lukulaite täytyy siis tunnistaa ennen tietojen lähettämistä. Yksinkertaisimmillaan tunniste sisältää avaimen ja se vastaa ainoastaan lukijalaitteelle joka lähettää sille ensin tämän avaimen. Tämä menetelmä on haavoittuvainen salakuuntelulle sillä niin avain kun tunnisteen sarjanumerokin lähetetään selväkielisenä. Parempi versio tästä toimintatavasta käyttää hash–funktiota tiedonsiirron salaamiseen. Tiedonsiirto alkaa lukijalaitteen kyselyllä. Tähän tunniste vastaa lähettämällä lukijalaitteelle MetaID:n, joka on laskettu hash–funktion avulla tiedonsiirron avaavasta avaimesta. Lukijalaite tarkistaa MetaID:n perusteella, mikä avain vastaa tätä tunnistetta ja lähettää löytämänsä avaimen tunnisteelle. Tunniste laskee hash–funktiolla tuloksen avaimesta ja vertaa tätä omaan MetaID:een. Mikäli arvot ovat samat, tunniste lähettää sarjanumeronsa lukulaitteelle. Näin lukulaite saadaan tunnistettua ja tunniste ei lähetä sarjanumeroaan lukulaitteille, joilla ei sen lukemiseen ole oikeutta.[8]

Heikkoutena tässä menetelmässä on se, että yksittäinen tunniste vastaa ensimmäiseen kyselyyn aina samalla tavalla. Vaikkakaan tämä MetaID ei sisällä tunnisteesta mitään varsinaista tietoa, voidaan sitä silti käyttää tunnisteen seuraamiseen.

2.5 Taajuusalueet ja tunnisteiden toimintaperiaate

Tunnisteiden ja lukulaitteiden välisessä tiedonsiirrossa RFID-tekniikassa on kaksi erilaista toimintaperiaatetta. Ne voivat toimia joko lähikentässä, jossa tiedon ja energian siirtoon käytetään muuttuvaa magneettikenttää tai kaukokentässä, jossa käytetään sähkömagneettista säteilyä [2]. Tunnisteen ja lukulaitteen toimintataajuus määrää samalla myös

toimintaperiaatteen. Matalilla taajuusalueilla toimivat tunnisteet käyttävät tiedonsiirtoon muuttuvaan magneettikenttää ja korkeammilla taajuusaluille toimivat tunnisteet käyttävät sähkömagneettista säteilyä.

Lähikentässä tunniste saa energiansa lukijan antennin muodostamasta magneettikentästä induktiivisesti. Tätä tekniikkaa käytetään lähinnä LF ja HF–taajuusalueilla suhteellisen pienillä lukuetäisyyksillä. Koska aallonpituus näillä taajuusalueilla on moninkertaisesti suurempi kuin lukijan antennin ja tunnisteen välinen etäisyys (125 kHz: 2400 m, 13.56 MHz: 22.1 m), sähkömagneettista kenttää voidaan käsitellä pelkästään muuttuvana magneettikenttänä. Tällöin tunnisteen antenni on periaatteessa kela ja sen koolla ei ole juuri vaikutusta käytettävään taajuuteen. Magneettikenttä heikkenee voimakkaasti siirryttäessä kauemmaksi antennista. Magneettikentän voimakkuus on $1/r^6$, missä r on etäisyys antennista [2].

Tiedonsiirto tunnisteesta lukijaan tapahtuu muuttamalla tunnisteen kelan kanssa sarjaan kytkettyä vastusta ajan kuluessa. Samalla muuttuu tunnisteen magneettikentästä induktanssin avulla ottama virta, joka näkyy myös lukijalaitteen antennin virran kulutuksen muutoksena [3]. Näin saadaan muutettua lukijalaitteen antennin kuormitusta ja voidaan käyttää tätä kuormituksen muutosta siirtämään tietoa tunnisteesta lukijaan. Tunniste muuttaa omaa resistanssiaan siirrettävän tiedon mukaisesti, ja lukijalaite havainnoi antenninsa käyttämän virran muutosta sekä tulkitsee sen mukaisesti tunnisteen lähettämän tiedon.

Kaukokentässä magneettikenttä ei enää ole dominoivassa asemassa, vaan tehon- ja tiedonsiirtoon käytetään sähkömagneettisia aaltoja. Tällöin tunnisteen antenni on yleensä muodoltaan dipoli, jonka pituus on puolet käytetystä aallonpituudesta. Antennin koko vaikuttaa käytettävään taajuuteen yleisesti niin, että mitä korkeampi taajuus, sitä pienempi antenni. Tästä syystä LF ja HF -taajuusalueiden tunnisteita ei voida käyttää tällä sähkömagneettiseen säteilyyn perustuvalla tekniikalla, sillä tällöin niiden antennin koko kasvaisi liian suureksi (yli 10 m 13.56 MHz taajuudella) [2].

Kaukokentässä myös tiedonsiirron toimintaperiaate on erilainen. Tietoa ei siirretä kuormitusta muuttamalla, vaan siihen käytetään takaisinsirontaa. Kun lukulaitteen lähettämä signaali saapuu tunnisteen antennille, tunnisteen antenni heijastaa osan lukulaitteen lähettämästä signaalista takaisin. Tunnisteen antennin impedanssia muutetaan ajan kuluessa ja näin toimittaessa heijastuksen voimakkuus vaihtelee. Näin toimittaessa voidaan heijastuksien avulla siirtää tietoa tunnisteesta lukijaan. Lukija vastaanottaa nämä heijastukset ja tulkitsee niistä lähetetyn viestin.[3]

2.5.1 Lähikenttä ja induktiivinen kytkentä

Induktiivista kytkentää käytettäessä tunniste muodostuu mikropiiristä ja antennina toimivasta kelasta. Nämä tunnisteet toimivat lähes aina passiivisesti. Tunniste saa toiminnassaan tarvitsemansa virran lukulaitteen antennin luomasta magneettikentästä, joka läpäisee tunnisteen antennina toimivan kelan. Näin kelaan indusoituu jännite, jota tunniste käyttää toiminnassaan. Kelan kanssa rinnan on kytketty kondensaattori, jonka arvo on asetettu niin, että tämän piirin värähtelytaajuus on sama kuin lukulaitteen lähettämän signaalin taajuus, jolloin kelaan indusoituva jännite saavuttaa maksimiarvonsa tällä taajuudella.[1]

Induktiivista kytkentää käytettäessä lukulaite ja tunniste toimivat muuntajan tapaan. Lukulaitteen antenni toimii ensiökelana ja tunnisteen antenni toisiokelana. Näin toisiokela ottaa energiaa magneettikentästä. Tämä huomataan lukulaitteen kelan kuormituksen muutoksena. Mikäli tunnisteen piiriin kytketään antennina toimivan kelan kanssa rinnan vastus, jota kytketään päälle ja pois, saadaan aikaan muutoksia lukulaitteen antennin impedanssissa. Nämä muutokset havaitaan myös lukulaitteessa ja niitä voidaan käyttää kuljettamaan tietoa.

Lukulaitteen kelan impedanssin muutokset ja samalla kelan jännitemuutokset ovat pieniä kelan jännitteeseen verrattuna ja näin ollen vaikeita havaita. Käytännössä 13.56 MHz järjestelmissä antennin syöttöjännite voi olla 100 volttia ja tiedonsiirtoon käytetty muutos noin 10 mV. Tämä jännitemuutos on niin pieni, että se on vaikea havaita ja tästä syystä tiedonsiirtoon käytetään amplitudimodulaation aikaansaamia sivukaistoja. Kun antennina toimivan kelan kanssa rinnan kytkettyä vastusta kytketään päälle ja pois suurella taajuudella f_s, syntyy kaksi spektriviivaa etäisyydelle $\pm f_s$ lukulaitteen lähetystaajuudesta f_{LUKIJA}. Syntynyttä signaalia kutsutaan apukantoaalloksi. Nämä apukantoaallot voidaan havaita myös lukulaitteessa ja niiden erottaminen on helppoa kaistanpäästösuotimien avulla.[1]

2.5.2 Kaukokenttä ja sähkömagneettinen kytkentä

Sähkömagneettista kytkentää käytetään UHF- ja mikroaaltotaajuuksilla. Näillä taajuuksilla induktiivisen kytkennän käyttäminen ei ole järkevää, sillä lukuetäisyydet jäisivät todella lyhyiksi. Toisaalta näillä korkeammilla taajuuksilla ei antennin koko kasva liian suureksi käytettäessä sähkömagneettista kytkentää. Passiivisilla tunnisteilla lukuetäisyyksiä rajoittaa lähinnä tunnisteen vastaanottaman energian määrä. Tunnisteen on saatava lukulaitteen signaalista tarpeeksi energiaa mikropiirinsä toimintaan. Passiivinen UHF–taajuusalueen tunniste pystyy toimimaan järkevillä lukulaitteen signaalinvoimakkuuksilla noin kolmen metrin etäisyydellä. Lukumatkaa pystytään kasvattamaan käyttämällä aktiivisia tunnisteita,

joissa mikropiirin tarvitsema virta otetaan sisäisestä paristosta ja tällöin ei tarvita niin vahvaa signaalia lukulaitteelta.[1]

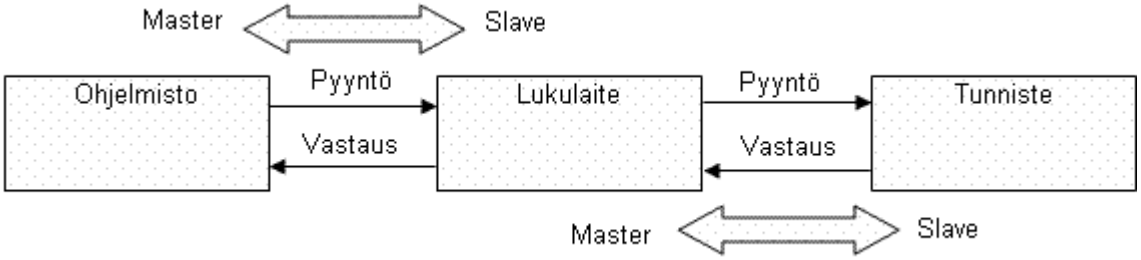
Sähkömagneettinen säteily heijastuu kohteista, jotka ovat kooltaan suurempia kuin noin puolet säteilyn aallonpituudesta. Mikäli kohde on resonanssissa säteilyn kanssa, se heijastaa säteilyä erityisen hyvin. Lukulaitteen antenni lähettää sähkömagneettista säteilyä teholla P_1. Pieni osa tästä tehosta päätyy tunnisteen antenniin tehona P'_1. Teho P_2, joka on osa tehosta P'_1, heijastuu tunnisteen antennista pois. Tällä kertaa osa tehosta P_2 päätyy lukulaitteen antenniin, jossa se voidaan havaita. Heijastumisen voimakkuutta voidaan säädellä muuttamalla antenniin kytkettyä kuormaa. Kun kuormaa kytketään päälle ja pois, muuttuu heijastunut teho P_2 ja samalla lukulaitteen vastaanottama osuus tehosta P_2. Näin voidaan siirtää tietoa tunnisteesta lukulaitteeseen.[1]

2.6 Törmäysten välttäminen

Kun lukulaitteen läheisyydessä on useita tunnisteita, ei niiden kaikkien kanssa voida keskustella samaan aikaan. Samaan aikaan lähetetyt signaalit törmäävät toisiinsa ja sotkeutuvat, jolloin niiden tulkitseminen on mahdotonta. Viestien vaihdon eri tunnisteiden kanssa on siis tapahduttava eri aikaan. Tämän saavuttamiseksi on kehitetty erilaisia törmäyksenestoalgoritmeja kuten eri muunnokset ALOHA – algoritmista ja puolitushaku [1]. ALOHA perustuu siihen, että sama viesti lähetetään useaan kertaan erilaisin väliajoin. Vaikka ensimmäisellä lähetyskerralla kaksi viestiä törmäisi, osuu niiden lähetys myöhemmin eri aikaan, ja viestien vastaanotto onnistuu. ALOHA on tehoton algoritmi ja siksi siitä onkin kehitetty parannettuja versioita kuten Frame Slotted ALOHA [4]. Puolitushaussa lukulaite lähettää tunnisteille sarjanumeron, johon tunnisteet vertaavat omaa sarjanumeroaan. Mikäli tunnisteen sarjanumero on pienempi tai yhtä suuri kuin kysytty sarjanumero, tunniste vastaa lukulaitteelle. Mikäli useampi kuin yksi tunniste vastaa, tapahtuu törmäys. Lukulaite havaitsee törmäyksen ja uusii kyselyn pienemmällä sarjanumerolla. Kun enää yksi tunniste vastaa, lukulaite on selvittänyt sen sarjanumeron ja voi aloittaa kommunikoinnin kyseisen tunnisteen kanssa.

3. TUNNISTEIDEN JA LUKULAITTEIDEN SISÄINEN RAKENNE

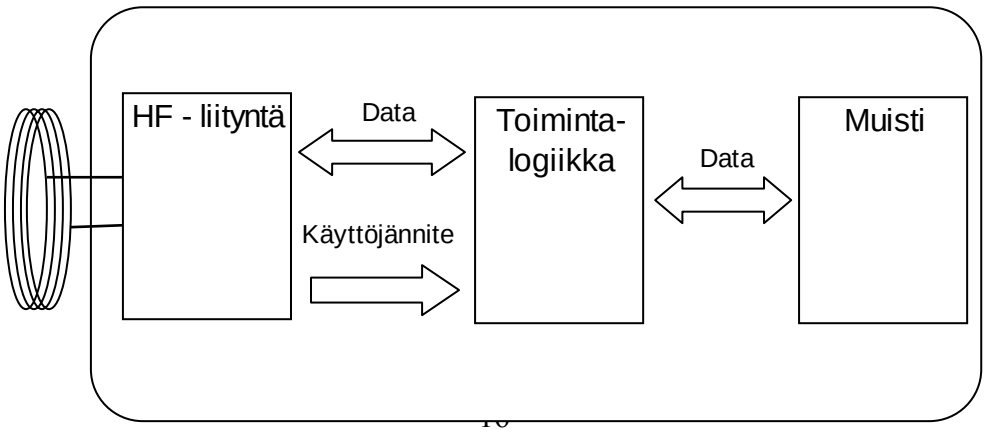
RFID-järjestelmä koostuu tunnisteesta, lukulaitteesta ja lukulaitetta käyttävästä ohjelmistosta. Ohjelmistolla ohjataan lukulaitetta, joka huolehtii tiedonsiirrosta tunnisteeseen ja takaisin. Kaikki toiminnot järjestelmässä seuraavat master–slave periaatetta. Ohjelmisto hallitsee lukulaitetta, joka hallitsee tunnistetta. Tiedonsiirto muodostuu pyyntö–vastaus–pareista. Ensin master lähettää aina pyynnön, johon slave vuorollaan vastaa. Tämä periaate on esitetty kuvassa kahdeksan.



Kuva 8. Tiedon kulku RFID-järjestelmässä

3.1 Tunnisteiden rakenne

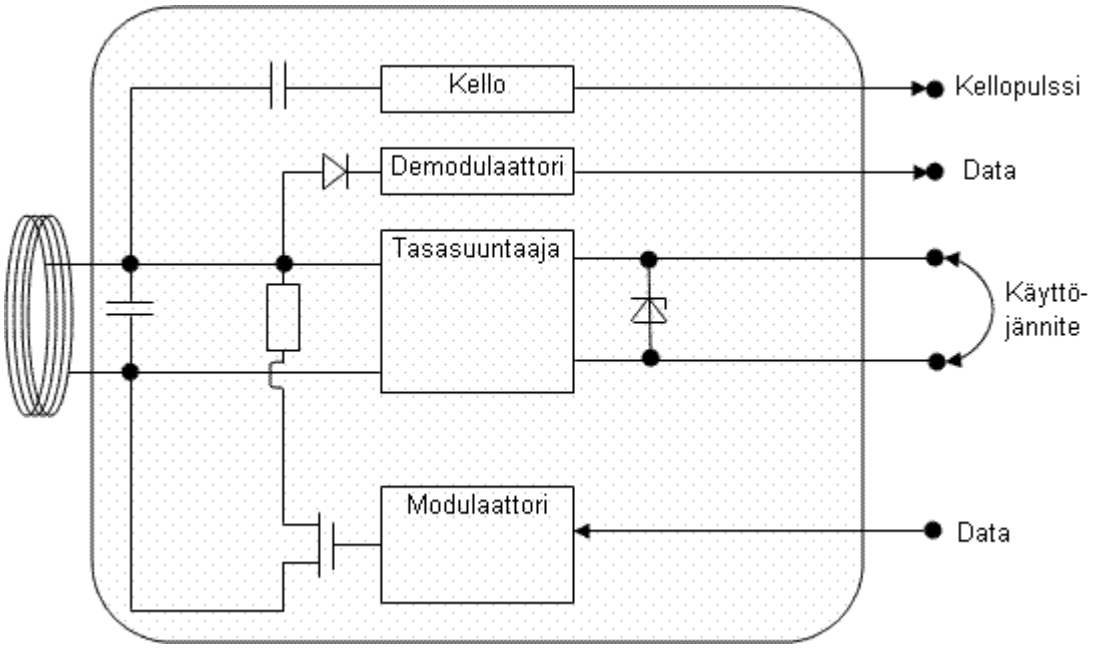
RFID-tunnisteiden sisäinen rakenne voidaan jakaa kolmeen pääosaan jotka nähdään kuvassa yhdeksän. HF–liityntä muuntaa ilmassa kulkevat signaalit tunnisteen toimintalogiikan ymmärtämään digitaaliseen muotoon sekä toisinpäin ja huolehtii passiivisten tunnisteiden käyttöjännitteen luomisesta. Toimintalogiikka ohjaa tunnisteen toimintaa. Se voi olla rakenteeltaan joko yksinkertainen tilakone, jolloin sen toiminta on piirin valmistusvaiheessa määrätty, tai mikroprosessori, jolloin se ajaa muistista lukemaansa ohjelmaa. Mikroprosessoria käytettäessä sama piiri voi toimia monissa erilaisissa tehtävissä, kunhan käytetään sopivaa ohjelmaa sen ohjaamiseen. Tunnisteen muistia käytetään eri tarkoituksiin. Se voi sisältää sekä pysyvää että käyttäjän muokattavissa olevaa tietoa. Pysyvä tieto voi olla mikroprosessorin ohjaukseen käytettävä ohjelma tai siihen voi olla tallennettuna tunnisteen pysyvä sarjanumero. Tämän lisäksi muistiin voidaan tallentaa käyttäjän tarvitsemaa tietoa.



Kuva 9. RFID tunnisteen sisäinen rakenne

3.1.1 HF-liityntä

HF-liityntä muodostaa rajapinnan analogisen, korkeataajuisen tiedonsiirtokanavan ja tunnistimen digitaalisten piirien välillä. Lukulaitteen luoma moduloitu HF-signaali demoduloidaan tunnisteessa ja näin luodaan tietovirta, jonka perusteella toimintalogiikka ohjaa tunnisteen toimintaa. HF-liityntä toteuttaa myös amplitudi- tai taajuusmodulaation tiedon siirtämiseksi tunnisteesta lukulaitteeseen. Passiivisissa tunnisteissa HF-liityntä lisäksi ottaa energiaa lukulaitteen luomasta sähkömagneettisesta kentästä. Tämä signaali tasasuunnataan, jonka jälkeen tunnisteen elektroniikka voi käyttää sitä käyttöjännitteenään. Kuvasta 10 nähdään esimerkki HF-liitynnän eri osista. Tämä piiri tuottaa kellopulssin joka tahdistaa tunnisteen toiminnan ja käyttöjännitteen RFID-tunnisteen eri osien käyttöön, sekä tarjoaa toiminnot tiedonsiirtoon niin lukulaitteelta tunnisteelle, kuin tunnisteelta lukulaitteellekin.

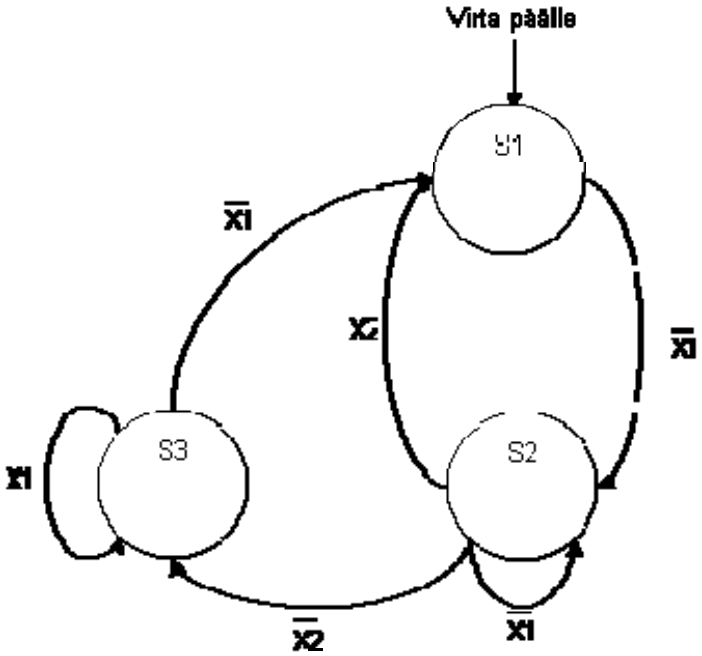


Kuva 10. HF-liitynnän osat

3.1.2 Toimintalogiikka

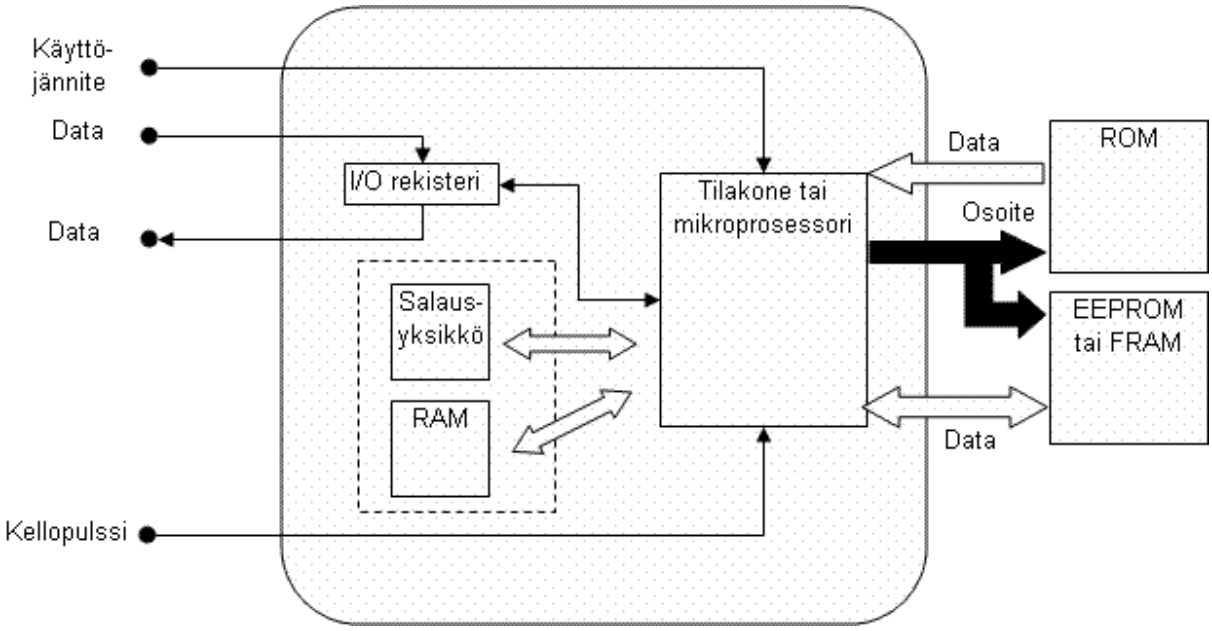
Tunnisteen toimintaa ohjaa toimintalogiikka. Yksinkertaisissa tunnisteissa siitä huolehtii tilakone. Kun tunniste saapuu lukulaiteen läheisyyteen, se luo lukulaitteen sähkömagneettisesta kentästä itselleen käyttöjännitteen. Tällöin tilakone siirtyy alkutilaan. Tiedonsiirto lukulaitteen kanssa kulkee I/O rekisterien kautta. Tunniste voi sisältää ROM muistia pysyville tiedoille sekä EEPROM tai FRAM muistia, jota voidaan muokata lukulaitteen ohjeiden mukaisesti. Mikäli tunniste mahdollistaa käyttäjien tunnistamisen tai

tiedon salauksen, tarvitaan tilakoneen lisäksi salaukseen oma yksikkönsä. Tilakoneeseen perustuvan tunnisteen toimintaa ei voida muuttaa muuten kuin muokkaamalla sen toteuttavan piirin rakennetta. Kuvassa 11 on esimerkki tilasiirtymäkaaviosta. S1, S2 ja S3 ovat laitteen mahdolliset tilat ja nuolilla on kuvattu ehdot, joilla siirtymät tilojen välillä tapahtuvat. Käytännössä siirtymät tilojen välillä tapahtuvat tunnisteen lukulaitteelta vastaanottamien käskyjen perusteella.



Kuva 11. Esimerkki tilakoneesta

Tilakoneen sijaan tunnisteen toimintaa voidaan ohjata myös mikroprosessorilla. Tällöin toimintalogiikkaa ei tarvitse toteuttaa mikropiiritasolla, vaan se toteutetaan ohjelmallisesti. Toiminnan muuttaminen vaatii tällöin ainoastaan ohjelmallisia muutoksia. Elektroniikan muutoksia ei tarvita. Mikroprosessoreina tunnisteissa käytetään yleisessä käytössä olevia mikroprosessoreita kuten 8051 ja 6805. Tämän lisäksi samalla piirillä voi olla apuprosessori tiedon salauksessa käytettävien laskutoimitusten suorittamiseksi. Mikroprosessori lukee toimintaohjeensa ROM muistiin tallennetusta ohjelmakoodista. ROM muistiin kirjoitettu ohjelmakoodi lisätään piirille sen valmistusvaiheessa niin sanotun maskiohjelmoinnin avulla, eikä sitä voida tämän jälkeen muuttaa. Kuvassa 12 nähdään tunnisteen toimintalogiikan periaatekuva. Toiminnan ydin on joko tilakone tai mikroprosessori. Näillä voi olla apunaan erillinen yksikkö tiedon salauksessa ja laitteiden tunnistamisessa käytettävien laskutoimitusten suorittamiseksi. Samoin mikroprosessori voi käyttää RAM muistia väliaikaisten tietojen tallentamiseksi. Pysyvät toiminnan ohjauksessa käytettävät tiedot on talletettu ROM muistiin. Käyttäjän tallettamat tiedot on talletettu tunnisteesta riippuen joko EEPROM tai FRAM muistiin.



Kuva 12. Tunnisteen toimintalogiikka

3.1.3 Muisti

Tunnisteet käyttävät erilaisia muistitekniikoita sekä pysyvän, että tilapäistenkin tietojen säilyttämiseen. Pysyvien tietojen tallentamiseen ROM (Read Only Memory) piireille voidaan valmistusvaiheessa käyttää valotusmaskeja tai laseria. Laserilla voidaan esimerkiksi tallentaa piirille yksilöllinen sarjanumero. Tiedon kirjoittamiseen valmiissa tunnisteessa voidaan käyttää RAM (Random Access Memory), EEPROM (Electrically Erasable Programmable ROM) tai FRAM (Ferroelectric RAM) muistipiirejä. Näistä vain EEPROM ja FRAM piirit soveltuvat tietojen pitkäaikaiseen tallentamiseen. RAM piirit vaativat jatkuvan käyttöjännitteen tai muuten niihin kirjoitettu ei säily.

RAM muistia käytetään tilapäisten tietojen tallentamiseen käskyjen suorittamisen aikana. RAM muistissa tieto säilyy ainoastaan niin kauan, kun se saa käyttöjännitteen. Tästä syystä sitä ei sellaisenaan voida käyttää tiedon pitempiaikaiseen säilyttämiseen. Tosin paristovarmennuksen avulla tämä on mahdollista.

EEPROM piirin toimintaperiaate perustuu kondensaattoriin. Kondensaattori pystyy säilyttämään varaustilansa pitkiäkin aikoja. EEPROM piirissä varautunut kondensaattori vastaa arvoa ”1” ja purkautunut kondensaattori arvoa ”0”. Arvon kirjoittaminen EEPROM-soluun vaatii suuren positiivisen tai negatiivisen jännitteen. EEPROM solun varaaminen vaatii noin 17 voltin jännitteen. RFID-tunnisteet tuottavat kuitenkin vain 3 tai 5 voltin jännitteen lukulaitteen sähkömagneettisesta kentästä, joten jännitettä on kohotettava

EEPROM piirin tarpeisiin. EEPROM solun varaamiseen kuluu aikaa 5-10 ms. EEPROM solun varauskertojen määrä on rajallinen, tyypillisesti 10000-100000, sillä joka kerta kun se varataan, elektroneja jää pysyväsi kondensaattorin oksidikerrokseen. Nämä elektronit vaikuttavat kynnysjännitteeseen ja lopulta muutos on niin suuri, ettei muistisolua voi enää käyttää.

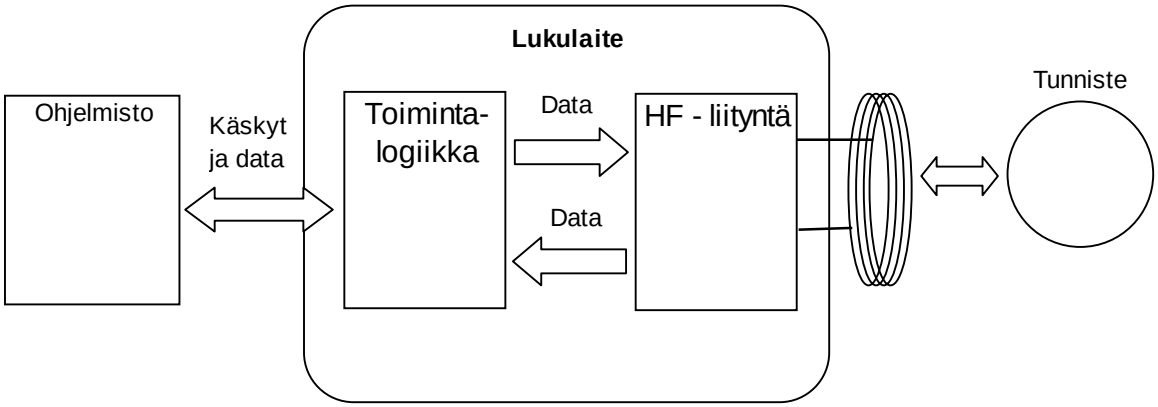
Varautunut kondensaattori menettää varaustaan hitaasti, mutta puolijohdevalmistajat lupaavat että tieto säilyy EEPROM piireillä kymmenen vuotta. Tätä aikaa voidaan pidentää kirjoittamalla tiedot muistiin uudelleen.

FRAM muistipiirien toiminta perustuu ferrosähköisyyteen, jossa aine säilyttää sähköisen polarisaationsa ilman sähkökentän vaikutusta. Tällaisessa elementissä on atomi, joka voi siirtyä kahteen eri paikkaan. Siirtyminen tapahtuu sähkökentän vaikutuksesta ja paikka säilyy tämän jälkeen vaikka sähkökenttä poistuisikin. Elementin arvon lukeminen tapahtuu sähkökentän avulla. Kun elementtiin kytketään jännite, muuttuu polarisaatio jännitteen mukaiseksi, mutta vapautuvan energian määrästä voidaan päätellä, mikä alkuperäinen tila oli. Lukemisen yhteydessä polarisaatio siis muuttuu aina lukujännitteen mukaiseksi, ja mikäli alkuperäinen tila oli toinen, on se kirjoitettava uudestaan.

Verrattuna EEPROM tekniikkaan FRAM muistien kirjoittaminen on todella nopeaa. Kirjoittaminen tapahtuu noin 0.1 µs ajassa verrattuna EEPROM piirin 5 – 10 ms aikaan. Samoin tarvittava jännite on huomattavasti pienempi, noin 2 volttia, ja samalla tarvittava energiamäärä on tuhansia kertoja pienempi. FRAM-piirien yhdistämisessä mikroprosessoreihin ja HF-liityntään on kuitenkin ongelmia, minkä vuoksi ne eivät vielä ole levinneet laajalle RFID käytössä.

3.2 Lukulaitteen rakenne

Vaikka RFID-järjestelmien toiminta vaihteleekin suuresti käytetyn taajuuden, kytkentätavan (induktiivinen/sähkömagneettinen) ja kommunikaation tyypin (full duplex, half duplex, vuoroittainen) mukaan, voidaan lukulaite jakaa kahteen pääosaan. Kontrollijärjestelmään ja HF liityntään. Nämä on esitetty kuvassa 13. Tämän lisäksi lukulaitetta yleensä ohjataan jonkinlaisella ohjelmistolla.



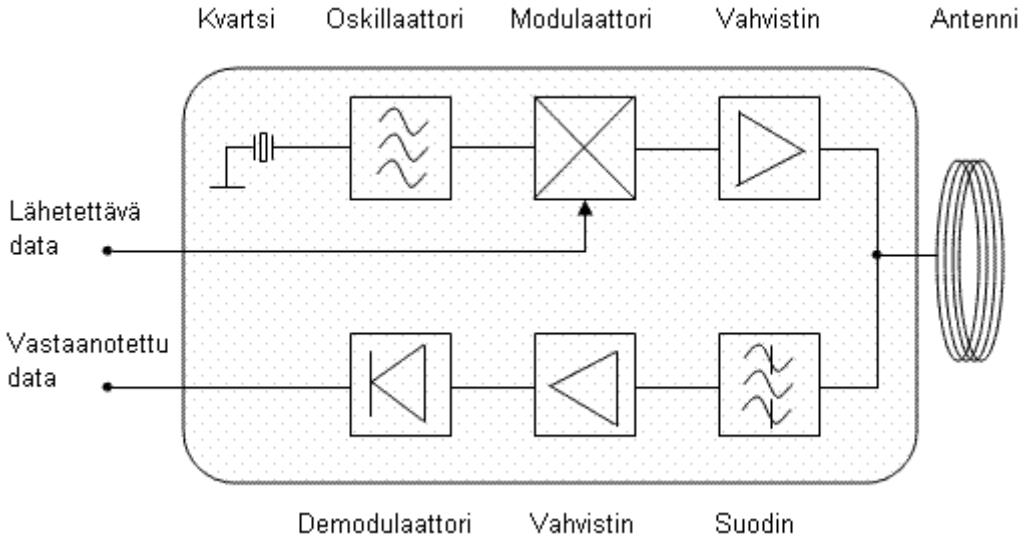
Kuva 13. Lukulaitteen pääosat ja liitynnät

3.2.1 HF - liityntä

Lukulaitteen HF liitynnällä on seuraavat tehtävät:

- Korkeataajuuksisen sähkömagneettisen kentän luominen passiivisten tunnisteiden virransyöttöä varten
- Tiedon lähettäminen tunnisteelle moduloimalla lähetettävää signaalia
- Tunnisteen lähettämän signaalin vastaanotto ja demodulointi

HF liityntä pitää sisällään kaksi erillistä signaalitietä, yhden lähetettävälle ja toisen vastaanotetulle signaalille. Kuvassa 14 on nähtävissä esimerkki induktiivista kytkentää käyttävän RFID lukulaitteen HF liittymän lohkokaaviosta.



Kuva 14. HF-liitynnän eri osat

Kuvassa nähdään kaksi signaalitietä, ylempi lähtevälle ja alempi saapuvalle signaalille. Lähtevän signaalin signaalitie alkaa kvartsioskillaattorista, jolla luodaan tarvittava toimintataajuus, esimerkiksi 13.56 MHz. Tämä taajuus syötetään modulaattoriin, jonne syötetään myös binääridataa sovitulla tavalla koodattuna (esim. Manchester tai NRZ). Modulaattori suorittaa joko amplitudi- tai vaihemodulaation ja näin yhdistää siirrettävän tiedon oskillaattorin luomaan signaaliin. Tämän jälkeen signaalia vahvistetaan sopivalle tasolle. Vahvistettu signaali syötetään antennille, joka lähettää sen ilmatien yli vastaanottavalle tunnisteelle.

Vastaanottopuolella antennilta saapuva signaali suodatetaan ensin kaistanpäästösuotimella. Tämän jälkeen suodatettu signaali vahvistetaan sopivalle tasolle ja syötetään demodulaattorille, joka erottaa signaalista tunnisteen lähettämän datan.

3.2.2 Kontrolliyksikkö

Lukulaitteen kontrolliyksiköllä on vähintään seuraavat tehtävät:

- Kommunikointi toimintaa ohjaavan ohjelmiston kanssa ja käskyjen vastaanotto tältä ohjelmistolta
- Tunnisteen kanssa tapahtuvan kommunikoinnin ohjaus
- Signaalin koodaus ja dekoodaus

Lisäksi kontrolliyksikkö voi suorittaa seuraavia tehtäviä:

- Törmäyksenhallinta-algoritmin suoritus
- Siirrettävän data salaaminen ja salauksen purku
- Autentikoinnin toteutus lukulaitteen ja tunnisteen välillä

Kontrolliyksikkö siis ohjaa lukulaitteen toimintaa ja sen toiminnasta on useimmiten vastuussa mikroprosessori. Prosessorin apuna saattaa olla erillinen prosessointiyksikkö salauksen vaatimien laskutoimitusten suorittamiseksi, mikäli lukulaitetta voi käyttää tällaisia toimintoja sisältävien tunnisteiden lukemiseen.

4. TUNNISTEIDEN STANDARDOINTI

RFID tunnisteita käytetään moniin eri tarkoituksiin. Tästä syystä tunnisteita onkin valmistettu usean eri standardin mukaan. Standardit vahvistaa kansainvälinen International Organization for Standardization (ISO). Standardien sisältö on tässä esitetty RFID Handbook [1] –kirjan mukaisesti.

4.1 Eläinten tunnistus (ISO 11784, 11785 ja 14223)

ISO standardit 11784, 11785 ja 14223 käsittelevät RFID järjestelmiä eläinten tunnistamiseen. Näiden standardien mukaisissa järjestelmissä käytetään passiivisia tunnisteita, jotka toimivat LF taajuusalueella, eli 134kHz taajuudella. Standardien sisältö on seuraava:

- ISO 11784: Eläinten RFID tunnistus – koodirakenne
- ISO 11785: Eläinten RFID tunnistus – tekninen toimintaperiaate
- ISO 14223: Eläinten RFID tunnistus – Kehittyneet tunnisteet
    - Osa 1: Ilmarajapinta
    - Osa 2: Koodin ja käskyjen rakenne
    - Osa 3: Sovellukset

Tunnisteiden fyysistä muotoa tai rakennetta ei ole määritetty näissä standardeissa ja näin ollen se voidaan suunnitella kullekin eläinlajille parhaiten sopivaksi.

4.1.1 Koodirakenne

Eläinten tunnistekoodi koostuu ISO 11784 standardin mukaan 64 bitistä eli kahdeksasta tavusta. Alla taulukosta yksi näkyy koodin tarkempi rakenne.

Taulukko 1. ISO 11784 koodirakenne

Bitin numero	Sisältö	Kuvaus
1	Eläin (1)/Ei eläin (0) sovellus	Kertoo käytetäänkö tunnistetta eläinten tunnistamiseen vai johonkin muuhun käyttötarkoitukseen

1 - 15	Varattu	Varattu tulevaisuuden käyttöä varten
16	Dataa (1)/Ei dataa (0)	Kertoo lähetetäänkö ylimääräistä dataa tunnistekoodin perässä
17 - 26	Maakoodi	Maakohtainen tunniste (ISO 3166 mukainen)
27 - 64	Yksilöllinen tunniste	Eläimen maakohtainen tunniste

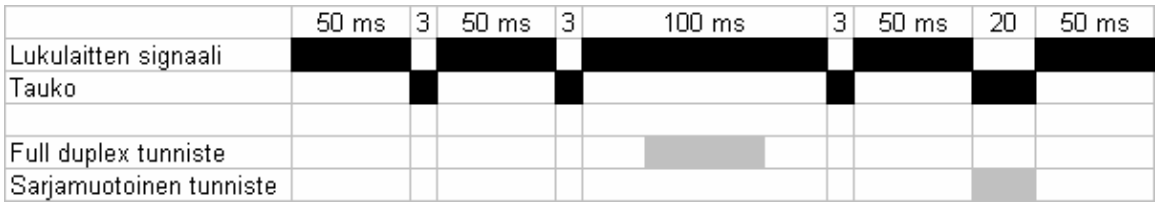
4.1.2 Tekninen toiminta

Standardin tavoitteena on mahdollistaa useiden valmistajien tunnisteiden ja lukulaitteiden yhteiskäyttö. Lukulaitteen on pystyttävä tunnistamaan erilaiset standardin mukaiset tunnisteet ja toimimaan niiden vaatimalla tavalla.

Lukulaitteen toimintataajuus on 134 kHz ± 1.8 kHz ja lukulaitteen lähettämä magneettikenttä toimii tunnisteen virtalähteenä. Kun lukulaitteen läheisyydessä ei ole tunnisteita tai tiedonsiirtoa ei muuten tapahdu, lähettää lukulaite 50 ms pituisia pulsseja, joiden välissä on 3 ms tauot. Tiedonsiirto voi tapahtua kahdella eri tavalla riippuen tunnisteen toimintaperiaatteesta.

Half/Full duplex tunniste lähettää tietonsa aina lukulaitteen pulssin aikana Tällöin pulssi voi kestää myös yli 50 ms, mikäli lähetys on 50 ms kohdalla vielä kesken. Pulssi voi tällöin kestää maksimissaan 100 ms.

Vuoroittaista tiedonsiirtoa käyttävän tunnisteen kanssa tiedon lähetys tunnisteesta lukulaitteeseen tapahtuu lukulaitteen signaalin tauon aikana. Tällöin tunniste alkaa lähettää tietojaan 3 ms pituisen tauon aikana. Mikäli lähetys ei ehdi valmiiksi 3 ms aikana, voidaan taukoa kasvattaa aina 20 ms pituuteen saakka. Kuva 15 esittää ISO 11785-tunnisteiden eri tiedonsiirtovaihtoehtoja.



Kuva 15. Tiedonsiirto ISO 11785 standardin mukaisten tunnisteiden ja lukulaitteen välillä

ISO 11785 mukaiset tunnisteet sisältävät ainoastaan yllä kuvatun tietosisällön, jota ei pysty muokkaamaan. Tunnisteiden tiedon muokkaamiseen ei siis ole olemassa käskyjä ja tiedonsiirto tapahtuu ainoastaan tunnisteesta lukulaitteeseen, ei koskaan toiseen suuntaan.

4.1.3 ISO 14223 – kehittyneet tunnisteet

ISO 14223 standardin mukaiset tunnisteet pohjautuvat ISO 11784 ja 11785 standardeihin, mutta ovat toiminnaltaan huomattavasti monipuolisempia. Niiden tietosisältöä pystytään muokkaamaan ja jopa suojaamaan muutoksilta.

ISO 14223 standardin tiedonsiirto on alaspäin yhteensopiva ISO 17885 standardin kanssa. ISO 14223 tunnisteiden tietosisältö on alkuosaltaan sama kuin ISO 17885 tunnisteillakin ja kummankin standardin mukaiset lukulaitteet voivat lukea tämän tunnistekoodin sekä ISO 14223 että ISO 17885 tunnisteista. Erona koodissa on bitti 16, joka kertoo sisältääkö tunniste muutakin tietoa kuin tämän koodin. Kun ISO 14223 lukulaite huomaa tämän bitin, se tietää, että tunnisteessa on muutakin tietoa ja se pystyy käsittelemään tätä tietoa standardin mukaisin komennoin. Tällöin se vaihtaa toimintatilaansa ISO 14223 mukaiseksi, jossa se pystyy lähettämään tunnisteelle standardin mukaisia komentoja. Tiedonsiirto tunnisteesta lukulaitteeseen tapahtuu samalla tavalla kuin ISO 17885 standardin mukaisten tunnisteidenkin kanssa.

Full duplex tunnisteilla vaihtaminen kehittyneeseen tilaan tapahtuu pitämällä 5 ms tauko 3 ms sijaan tai lähettämällä 5 bittisen vaihtokomennon. Tämän jälkeen voidaan tunnisteeseen lähettää käskyjä.

Sarjamuotoista tiedonsiirtoa käyttävää tunnistetta ei tarvitse erikseen vaihtaa toiseen tilaan vaan komennot voidaan lähettää lukulaitteen 50 ms pituisen signaalin loppuosassa vapaasti. Tällöin tunniste vastaa seuraavalla lukulaitteen tauolla. Mikäli lukulaite ei lähetä käskyjä, tunniste vaihtaa toimintansa takaisin ISO 17885 standardin mukaiseksi.

Taulukossa 2 on kuvattu ISO 14223 käskyn rakenne. Varsinainen käsky ilmaistaan viidellä bitillä ja näin ollen erilaisia käskyjä voi olla maksimissaan 32 kappaletta. Käskykoodit 0-19 on määritelty standardissa ja numerot 20–32 ovat vapaasti käytettävissä valmistajan omiin tarkoituksiin.

Taulukko 2. ISO 14223 käskyn rakenne

Liput	Käsky	Parametrit	Data	CRC
4 bittiä	5 bittiä	6 - 76 bittiä	32 bittiä	16 bittiä

Käskyn saatuaan tunniste lähettää vastauksen, jonka rakenne on kuvattu taulukossa 3. Vastauksen ensimmäinen bitti kertoo tapahtuiko käskyä suorittaessa virhe vai ei ja samalla sen, sisältääkö vastausviesti virhekoodin vai ei. Onnistuneen käskyn jälkeinen vastaus voi sisältää tietoa, mikäli kyseessä oli tiedon lukukäsky. Yksinkertaisimmillaan vastaus on vain yhden bitin mittainen.

Taulukko 3. Vastauksen rakenne

Virhelippu	Data/Virhekoodi	CRC
1 bitti	3 - 32 bittiä	16 bittiä

4.2 Kontaktittomat älykortit (ISO 10536, 14443 ja 15693)

Kontaktittomille älykorteille on olemassa kolme eri ISO standardia, ISO 10536, 14443 ja 15693. Pääasiallisena erona näillä on etäisyys, jolla lukemisen on suunniteltu tapahtuvan. Taulukossa 4 on listattu näiden tunnisteiden lukuetäisyyksiä.

Taulukko 4 Kontaktittomien älykorttien suunnitellut lukuetäisyydet

Standardi	Lukuetäisyys
ISO 10536	0 -1 cm
ISO 14443	0 - 10 cm
ISO 15693	0 - 1 m

4.2.1 ISO 10536

ISO 10536 käsittelee kontaktittomia älykortteja, joiden lukuetäisyys on alle yhden senttimetrin. Näiden älykorttien lukemiseen käytetään lukulaitteita, joiden sisään kortti asetetaan samaan tapaan kuin muutkin älykortit. Näiden korttien korkeat valmistuskustannukset ja vähäiset hyödyt verrattuna kontaktin vaativiin älykortteihin ovat vähentäneet näiden älykorttien kysyntää.

Käyttötarkoituksesta johtuen standardi määrittelee tunnisteiden fyysiset mitat samoiksi kuin kontaktillisissakin älykorteissa. Standardi määrittelee myös alueet kortissa, joissa tiedonsiirtoon käytettävät induktiiviset ja kapasitiiviset komponentit sijaitsevat. Näiden sijoittelu on sellainen, että kortti voi olla lukulaitteessa miten päin tahansa.

4.2.2 ISO 14443

ISO 14443 standardi käsittelee älykortteja joiden lukuetäisyys on tyypillisesti joitakin senttejä. Käyttötarkoituksena näillä tunnisteilla on esimerkiksi pääsyliput.

Tunnisteet saavat virtansa lukulaitteen 13.56 MHz taajuudella lähettämästä signaalista. Signaalin vastaanottamiseksi tunnisteessa on suurikokoinen kela, jossa on tyypillisesti 3 – 6 kierrosta kuparilankaa. Käytännössä lukuetäisyyksiä rajoittaa tunnisteen vastaanottama energiamäärä, jonka on oltava riittävä sen toiminnan varmistamiseksi.

ISO 14443 tunnisteiden ja lukulaitteen väliseen tiedonsiirtoon on olemassa kaksi eri toimintatapaa, A ja B. Tunniste itsessään tukee näistä vain toista, mutta lukulaitteen tulee osata toimia kummankin tyyppisten tunnisteiden kanssa oikealla tavalla.

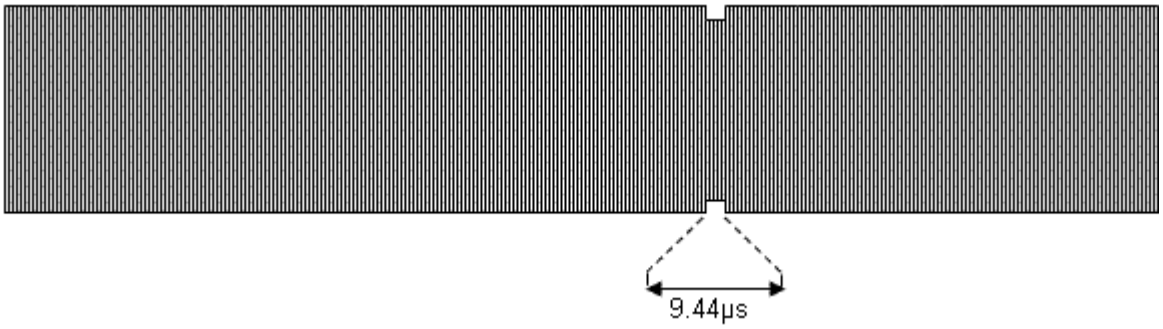
Tyypin A tunnisteen kanssa kommunikoitaessa käytetään 100 % amplitudimodulaatiota ja muunnettua Miller koodausta bittien esittämiseen. Signaalin muutos on aina 100 % eli signaali on aina joko päällä tai pois. Jotta virran siirto tunnisteeseen pysyisi riittävän vakaana, on signaalin poissaoloaika ainoastaan 2–3 μs. Tiedonsiirto tunnisteesta lukulaitteeseen tapahtuu kuormitusta muuttaen käyttäen apuna 847 MHz apukantoaaltoa. Tieto lähetetään kytkemällä apukantoaaltoa päälle ja pois käyttäen Manchester koodattua bittijonoa.

Tyypin B tunnisteen kanssa tiedon siirtoon lukulaitteesta tunnisteeseen käytetään 10 % amplitudimodulaatiota ja yksinkertaista NRZ koodaustapaa bittien esittämiseen. Tällöin signaalin voimakkuus lähettäessä arvoa ”1” on arvossa 100 % ja lähettäessä arvoa ”0” se on 90 % maksimista. Tiedonsiirrossa tunnisteesta lukulaitteeseen käytetään 180° vaihemodulointia 847 kHz apukantoaallolla ja NRZ koodatulla lähetettävällä bittijonolla.

4.2.3 ISO 15693

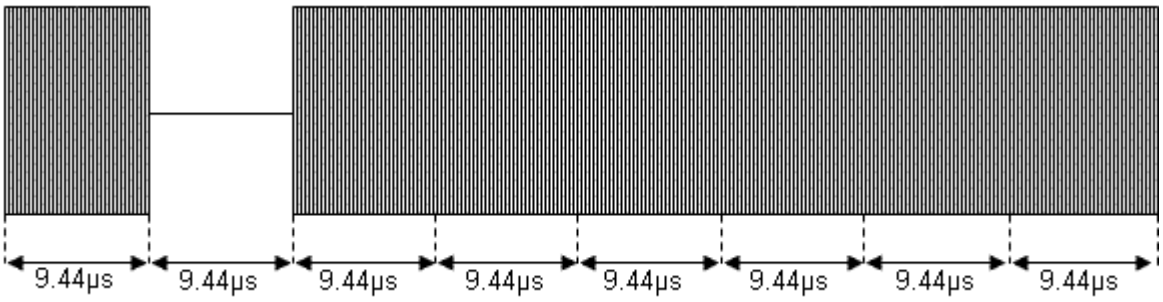
ISO 15693 määrittelee kontaktittomien älykorttien, joiden lukuetäisyys on jopa metri, ominaisuudet. Tunnisteiden fyysisiksi mitoiksi standardi määrittelee samat kuin muillakin älykorteilla, mutta toiminnaltaan ISO 15693 standardin mukaisia tunnisteita on saatavana monen muotoisina ja kokoisina.

Tunnisteen virtalähteenä toimii lukulaitteen muodostama 13.56 MHz taajuudella toimiva magneettikenttä. Kommunikoinnin onnistuminen vaatii, että tunniste pystyy luomaan lukijan magneettikentästä tarpeeksi virtaa toimintansa mahdollistamiseksi. Tiedonsiirtoon lukulaitteelta tunnisteelle on useita eri vaihtoehtoja. Ensinnäkin on mahdollista käyttää joko 10 % tai 100 % amplitudimodulaatiota. Toisekseen tiedon koodaukseen on kaksi mahdollisuutta: 1:256 tai 1:4. Ensimmäisessä tavassa kerralla lähetetään 8 bittiä eli yksi tavu. Sen lähettämiseen käytetään 512 9,44 μs pituista aikalohkoa ja näin ollen tavun lähettämiseen kuluu aikaa 4.833 ms. Kuvassa 16 nähdään 10 % amplitudimoduloitu 1:256 tyyppinen signaali.



Kuva 16. 10 % amplitudimoduloitu 1:256 tyyppinen signaali

Toisessa tavassa kerralla lähetetään vain kaksi bittiä. Tämän lähettämiseen tarvitaan kahdeksan 9,44 µs pituista aikalohkoa ja näin ollen tavun lähettämiseen kuluu aikaa 75.52 µs. Esimerkki tästä nähdään kuvassa 17.



Kuva 17. 100 % amplitudimoduloitu 1:4 tyyppinen signaali

Jälkimmäinen, 1:8 tyyppinen, tapa on siis nopeampi, mutta koska ensimmäisessä tavassa lukulaitteen lähettämä magneettikenttä on ”päällä” suuremman osan ajasta, mahdollistaa se suuremmat etäisyydet lukulaitteen ja tunnisteen välillä. Pitkiä etäisyyksiä tarvittaessa kannattaa myös käyttää 10 % amplitudimodulaatiota, sillä tällöin lukulaitteen signaalista saadaan pienimmilläänkin 90 % maksimitehosta, eikä se tipu koskaan nollille. Näin ollen voidaan tunnisteen tarvitsema virta saada lukulaitteen magneettikentästä hieman kauempaa kuin 100 % amplitudimodulaatiolla.

Tiedonsiirto tunnisteesta lukijaan tapahtuu muuttamalla tunnisteen magneettikentälle aiheuttamaa kuormaa. Tunnisteessa sijaitsevaa kuormaa kytketään päälle ja pois alikantoaallon tahdissa. Alikantoaaltoa moduloidaan Manchester-koodatun syötteen mukaisesti joko amplitudi tai taajuusmodulaatiolla. Lukulaite ilmoittaa tunnisteelle kumpaa modulointitapaa käytetään.

4.3 Electronic Product Code (EPC)

Electronic product code (EPC) on EPCglobal Inc:in [19] tuotteiden tunnistamiseen kehittämä RFID-standardi joka on sittemmin otettu osaksi ISOn 18000-6 standardia joka käsittelee UHF-taajuusalueen RFID-tunnisteiden ja lukulaitteiden välistä kommunikaatiota.

EPC on koodi, jolla on tarkoitus tunnistaa kaikki mahdolliset tuotteet hyödyntäen RFID–tekniikkaa tai mahdollisesti jotakin muuta tunnistustekniikkaa. Jokaiselle tuotteelle siis annetaan oma koodi, jolla se voidaan erottaa kaikista muista tuotteista. Standardien tunnistetietojen lisäksi EPC–tunniste voi pitää sisällään myös muuta, käyttäjän määräämää tietoa. EPC–standardit määrittelevät tunnisteen sisältämien tietojen pituudet, mutta eivät sen sisältöä.

Varsinainen tunnistetieto voi olla koodattuna useammalla eri tavalla. Tunnisteen sisältämät tiedot alkavat aina otsikkokentällä, jonka sisältö määrää sitä seuraavan tiedon formaatin. Tunnistetieto voi olla joko kaksi tai kahdeksan bittiä pitkä. Kahdella bitillä voidaan ilmaista ainoastaan kolme eri formaattia, sillä arvo nolla on varattu pidemmille otsikkokentille. Samalla periaatteella kahdeksan bitin otsikkokentällä voidaan ilmaista 63 eri formaattia. Kaksi ensimmäistä bittiä ovat aina nollia ja kokonaisarvo nolla on varattu vielä pidemmille otsikkokentille, mikäli niitä aletaan käyttää tulevaisuudessa.

Tällä hetkellä eri formaatteja on määritelty 13 kappaletta. Näissä formaateissa tunnisteen sisältämän tiedon pituus voi olla 64 tai 96 bittiä. Sen lisäksi osa formaateista on varattu tulevaisuutta varten suuremmille tiedon pituuksille.

Otsikkokentän jälkeen joissakin formaateissa käytetään lisätietoa, jonka avulla voidaan tunnistaa, minkä tyyppisestä tuotteesta tai pakkauksesta on kysymys. Näin voidaan lukuvaiheessa erotella esimerkiksi yksittäiset tuotteet ja suuremmat pakkaukset, joiden sisällä on useita yksittäisiä tuotteita. Esimerkiksi kun varastoon saapuu kuormalava täynnä tuotteita ja sekä kuormalavassa että kaikissa tuotteissa on RFID-tunniste, voimme lukea pelkästään kuormalavan tiedot ilman että meidän tarvitsee lukea kaikkien yksittäisten tuotteiden tietoja.

Esimerkkinä EPC–koodista toimii general identifier GID-96 –koodi. Se on 96 bittinen koodi, jossa on otsikkokentän lisäksi kolme muuta kenttää: g*eneral manager numbe*r, *object glass* sekä *serial number.* Näistä general manager number kertoo, mikä taho on vastuussa koodista. Se voi olla esimerkiksi tuotteen valmistaja tai muu taho, joka on lisännyt koodin tuotteeseen. Object class kertoo, minkälaisesta tuotteesta on kysymys, se voi olla tuotteen malli tai jokin laajempi luokittelu tyypin mukaan. Viimeinen kenttä eli serial number yksilöi tämän tietyn tuotteen sen luokan sisällä. Yhteenveto kenttien sisällöstä nähdään taulukosta 5. Yhdessä

nämä kentät yksilöivät tuotteen täydellisesti. Kahdella tuotteella ei voi olla samaa tunnistekoodia.

Taulukko 5. General Identifier – koodin formaatti

Kenttä	Header	General Manager Number	Object Class	Serial Number
Pituus (bittiä)	8	28	24	36
Arvo	0011 0101 (Binäärinä)	268 435 455 (Maksimi desimaaliarvo)	16 777 215 (Maksimi desimaaliarvo)	68 719 476 735 (Maksimi desimaaliarvo)

Header kenttä kertoo, että kyseessä on juuri GID-96 tyyppinen koodi. Kolme muuta kenttää sisältävät kokonaislukuja, joilla tunnistetaan koodin myöntänyt taho, esineen tyyppi ja esineen sarjanumero. Kokonaisluvun pituus ja samalla maksimiarvo vaihtelee kentästä toiseen. General manager Number kentän pituus on tällä koodityypillä 28 bittiä, object class kentän pituus on 24 bittiä ja serial number kentän pituus on 36 bittiä.

5. YKSITYISYYS JA TIETOTURVA

RFID-tunnisteita käytetään monenlaisiin käyttötarkoituksiin. Tunnisteiden sisältämät tiedot saattavat olla sellaisia, että niiden asiaton lukeminen tai muokkaaminen olisi syytä estää. Tunnisteen tietosisällön lukemisen estämisellä voidaan estää tunnisteen kopiointi. Tietosisällön muokkaamisen estäminen on tärkeää esimerkiksi RFID–tekniikkaa hyödyntävissä pääsylipuissa, jotta lipun käyttäminen useaan kertaan estetään.

Lukemisen ja muokkaamisen estämisen tarkoituksena on yleensä tunnisteita hyödyntävien tahojen etujen suojaaminen. Toinen ryhmä, joka on tunnisteita käytettäessä otettava huomioon, on yksityishenkilöt, joiden haltuun tunnisteet tai tunnisteita sisältävät tuotteet lopulta päätyvät. Loppukäyttäjien osalta on otettava huomioon heidän yksityisyytensä suojaaminen. Koska RFID-tunnisteet voidaan etälukea ilman näköyhteyttä, mahdollistavat ne tunnisteiden ja sitä kautta tunnisteen omistavan henkilön seuraamisen.

5.1 Yksityisyys

RFID tekniikan avulla voidaan tunnistaa automaattisesti erilaisia kohteita, kuten tuotteita tai ihmisiä. Automaattista tunnistusta voidaan käyttää ihmisten seurantaan, tai niiden avulla voidaan saada hankittua ihmisten henkilökohtaisia tietoja. Tästä syystä yksityisyyden suoja on otettava huomioon RFID järjestelmiä suunniteltaessa. Yksityisyyden käsite ei ole yksiselitteinen ja eri ihmiset tarkoittavat osittain eri asioita siitä puhuessaan. Perinteisesti yksityisyydestä puhuttaessa on tarkoitettu seuraavia asioita[9]:

- Se on ihmisen perusoikeus, johon kuuluu vapaus perusteettomista etsinnöistä ja takavarikoista tai tungettelusta.

- Henkilökohtaisten tietojen suojaus

Henkilökohtaisille tiedoille on luotu useita eri määritelmiä niin tahojen toimesta kuin lainsäädännössäkin (EU, maakohtaiset lait, OECD ohjeet…).

70–luvulla pelot yksityisyyden menettämiseen suuntautuivat suuriin tietokantoihin, jotka sisälsivät ihmisten henkilökohtaisia tietoja [9]. Nykyään näiden tietokantojen rinnalle on noussut Internet, jossa hakukoneiden avulla on helppo yhdistellä eri tiedonpalaset toisiinsa ja näin voidaan kerätä tietoja ihmisistä. RFID-tekniikka luo juuri tällaisia tiedon palasia. Yleensä tiettyyn tuotteeseen kytketyn RFID-tunnisteen tiedot eivät itsessään kerro mitään sen omistavasta ihmisestä, mutta sen tietojen avulla voidaan päästä käsiksi henkilökohtaisiin tietoihin.

RFID-tunnisteet voivat sisältää suoraan henkilökohtaisia tietoja kuten vaikka RFID-tunnisteen sisältävä niin sanottu biopassi tai työntekijän henkilökortti. Näitä on helppo käyttää henkilön seurantaan. Toisaalta lemmikkieläimen RFID-implantti sisältää tietoja sen omistajasta ja näin lemmikkiä seuraamalla voidaan suurella todennäköisyydellä seurata myös sen omistajaa. Tämän lisäksi henkilöiden seurantaan voidaan käyttää RFID-tunnisteita joita ei alun perin ole mitenkään kytketty omistajaansa. Esimerkiksi jokin vaate voi sisältää RFID-tunnisteen. Kun tunniste on kiinnitetty vaatteeseen, ei vielä tiedetä mitään sen tulevasta omistajasta, mutta sen jälkeen kun vaate on otettu käyttöön, voidaan luoda linkki vaatteen tunnisteen ja sen omistajan välillä ja näin saada lisätietoja omistajan liikkeistä.

RFID-teknologian suurin ongelma yksityisyyden kannalta on se, että RFID-tunnisteet voidaan lukea langattomasti, niin ettei tunnisteen omistaja huomaa mitään tapahtuneen. Näin ollen täysin vieras henkilö voi halutessaan selvittää, mitä tunnisteilla varustettuja tuotteita jollakin henkilöllä on mukanaan ja mahdollisesti käyttää saamiaan tietoja edelleen henkilön vakoilemiseen. Mikäli käytettävissä olisi useita lukulaitteita eri paikkoihin sijoitettuna, voidaan tunnisteiden avulla seurata niiden omistajan liikkeitä. Kun tunnisteen sarjanumero on yhdistetty sen omistajan tietoihin, tiedetään aina kun sama sarjanumero luetaan, missä omistaja on fyysisesti.

RFID-teknologia mahdollistaa seuraavat kolme yksityisyyden uhkaa:

- Profilointi
    - Lukijaverkko voi helposti ja edullisesti kerätä tietoa henkilöiden mukana kulkevista tunnisteen sisältävistä tuotteista ja lisätä nämä tiedot heidän henkilökohtaisiin profiileihin.
- Valvonta
    - Ihmisen sijaintia voidaan valvoa hänen mukanaan kuljettamien tunnisteen sisältävien tuotteiden avulla. Parhaiten valvonta onnistuu, mikäli henkilöllä on jokin henkilökohtainen tunniste, kuten ajokortti tai passi. Henkilön sijaintia voidaan seurata myös hänen mukanaan kuljettamien muitten tunnistein varustettujen tuotteiden avulla, kunhan aikaisemmin on luotu linkki tuotteen ja sen omistajan välille.
- Toiminta
    - RFID-tekniikan avulla henkilö voidaan tunnistaa ja tunnistaminen tietyssä maantieteellisessä paikassa voi laukaista jonkin toiminnon.

Toiminto voi olla vaikkapa pidättäminen viranomaisten taholta tai kohdennettujen mainosten näyttäminen mainostajien toimesta.

Toimiakseen käytännössä profilointi ja valvonta vaativat linkin luettujen tunnisteiden ja niiden omistajan välillä. Eli profilointia ei voi suorittaa mikäli ei tiedetä kenen ostoksia luetaan ja pelkän tunnisteen seuraaminen on turhaa, mikäli ei tiedetä kuka sen omistaa tai kuka sitä kantaa mukanaan. Toiminta taas ei välttämättä vaadi tätä linkkiä. Esimerkiksi kohdennettuja mainoksia voidaan näyttää ihan hyvin henkilön mukanaan kuljettamien tuotteiden perusteella vaikka henkilön nimeä ei tiedetäkään.[9]

5.1.1 Tekniikat yksityisyyden suojaamiseksi

Kuten edellä selvisi, voidaan RFID-teknologiaa käyttää monella tapaa loukkaamaan käyttäjänsä yksityisyyttä. Tästä syytä onkin kehitetty erilaisia menetelmiä, jolla tunnisteen luvaton lukeminen voidaan estää ja näin varjella tunnisteen omistajan yksityisyyttä.[10]

5.1.2 Tunnisteen ”tappaminen”

Joillekin tunnisteille on mahdollista antaa käsky, jolla ne ”tappavat” itsensä. Tämän jälkeen tunniste ei toimi enää millään lailla, eikä sitä ole mahdollista herättää uudestaan henkiin. Tämän menetelmän tarkoituksena on, että kun kuluttaja on ostanut ja maksanut RFID-tunnisteella varustetun tuotteen, tunniste tapetaan. Tappokäsky vaatii itse käskyn lisäksi salasanan, jolla estetään luvaton tunnisteen tuhoaminen. Kun tunniste on tuhottu, ei sitä voi enää havaita lukulaitteella ja näin ollen kuluttajan yksityisyys ei ole enää uhattuna.

Tunnisteen tuhoamisen huonona puolena on, että tuhoamisen jälkeen tunnistetta ei voida enää käyttää. Automaattiselle tunnistukselle olisi kuitenkin käyttöä vielä senkin jälkeen kun tuote on poistunut kaupasta. Esimerkiksi tulevaisuuden älykkäät jääkaapit ja mikroaaltouunit voisivat tunnistaa sisällään olevat tuotteet ja säätää toimintaansa löytämiensä tietojen mukaan. Jääkaappi voi varoittaa tietyn tuotteen loppumisesta tai vanhenemisesta ja mikroaaltouuni voi valita oikean kypsennysohjelman tunnistamalleen ruoalle automaattisesti. Kauppaa taas tunniste kiinnostaa esimerkiksi siinä tapauksessa että tuote palautetaan vaikkapa viallisena. Tunnisteen avulla kaupan ja valmistajan on helpompi selvittää syitä vikaan ja parantaa näin toimintaansa.

5.1.3 Faradayn häkki

Faradayn häkki on metallista valmistettu esine, joka estää sähkömagneettista säteilyä kulkemasta sen ulkopuolelta sisäpuolelle ja päinvastoin. Se voi olla rakennettu vaikkapa metallikalvosta tai verkosta. Faradayn häkin sisällä olevaa RFID-tunnistetta ei voida lukea häkin ulkopuolelta. Myymälävarkaiden tiedetäänkin käyttäneen foliolla vuorattuja laukkuja välttääkseen varkauden estoon tarkoitettujen tunnisteiden lukemisen myymälän porteilla.

Faradayn häkki ei sovellu kaikkien RFID-tunnisteiden lukemisen estämiseksi, sillä tunniste pitäisi saada häkin sisään. Mikäli tunniste on kiinnitettynä suureen esineeseen tai jopa ihmiseen on tämä käytännössä hyvin vaikeaa.

5.1.4 Aktiivinen radiohäirintä

Aktiivisessa radiohäirinnässä käytetään radiolähetintä, joka lähettää jatkuvasti sellaista signaalia, joka sotkee RFID-lukulaitteen ja tunnisteen välisen liikenteen. Signaalit siis törmäävät ja näin ollen lukulaite ei pysty havaitsemaan läheisyydessään sijaitsevia tunnistimia.

Tällainen lukemisen esto sotkee kaiken lähettimen kantomatkan sisäpuolella olevan samalla taajuudella toimivan tiedonsiirron hallitsemattomasti ja näin ollen ei ole järkevä toimintatapa tunnisteiden luvattoman lukemisen estämiseksi. Aktiivisen radiohäirinnän sijaan tunnisteiden lukemisen estämiseen kannattaa käyttää hienostuneempia tapoja, jotka eivät häiritse muuta tietoliikennettä

5.1.5 Älykkäät tunnisteet

Tunnistimien luvatonta lukemista voidaan myös estää käyttämällä ”älykkäitä” tunnistimia, jotka eivät paljasta sarjanumeroaan kaikille lukulaitteille, vaan ainoastaan silloin, kun sarjanumeron lukeminen on luvallista. Tunnisteet voidaan lukita salasanalla, jolloin ne eivät kerro sarjanumeroaan yhdellekään lukulaitteelle, ennen kuin ne on avattu oikealla salasanalla. Tunnisteiden ja lukulaitteen välinen tiedonsiirto voi myös olla salattu yhteisellä salausavaimella.

Näiden menetelmien huono puoli on tarvittavien tunnistimien hinta. Koska tunnisteet ovat toiminnaltaan huomattavasti tavallista monimutkaisempia, ovat ne myös selvästi kalliimpia. Toisaalta näissä menetelmissä tarvitaan aina jonkinlaista avainten hallintaa. Tämä tekee näistä järjestelmistä huomattavasti monimutkaisempia ja vaikeampia käyttää. Näistä syistä johtuen

älykkäiden, salausfunktioilla varustettujen, tunnisteiden käyttäminen ei sovellu kaikkiin tarkoituksiin.

5.1.6 Blocker Tag

Blocker Tag on tunniste, joka estää tunnisteiden lukemisen sekaantumalla tunnisteiden etsimiseen esiintymällä kaikilla mahdollisilla sarjanumeroilla [10]. Käytettäessä puolitushakua blocker tag vastaa hakuavaruuden jakamisvaiheessa avaruuden kummallakin puolella. Näin lukulaite joutuu käymään koko hakuavaruuden läpi ja se luulee löytävänsä tunnisteen jokaisella mahdollisella sarjanumerolla. Käytännössä hakuavaruuden läpikäyminen ei onnistu järkevässä ajassa, vaan kun blocker tag käy lukulaitteen läheisyydessä, lukulaite tuhlaa aikansa turhaan.

Blocker tag ei välttämättä esiinny kaikkina nimiavaruuden tunnisteina, vaan se voi toimia myös rajatummalla alueella. Näin ollen se ei välttämättä estä lukulaitteen toimintaa kokonaan, vaan se ainoastaan estää tiettyjen tunnisteiden sarjanumerojen lukemisen. Tosin järkevästi toimiakseen tunnisteen on tällaisessa tapauksessa pystyttävä ilmoittamaan, että tietty osa nimiavaruudesta on blokattu eikä sen lukeminen onnistu, jotta lukulaite osaa siirtyä lukemaan muita tunnisteita. Muuten lukulaite saattaa tuhlata aikansa blocker tagin estämän nimiavaruuden kanssa, vaikka sen lähettyvillä olisi muitakin tunnisteita, jotka se pystyisi lukemaan.

5.2 Tietoturva

RFID-järjestelmät eivät ole ongelmattomia tietoturvan osalta. Yksinkertaisten tunnisteiden tietosisällön voi lukea kuka tahansa, jolla on hallussaan lukemiseen soveltuva laite. Suurimmassa osassa tunnisteita on yksilöllinen sarjanumero, jota ei tunnisteen valmistamisen jälkeen pysty muokkaamaan. Muiden tunnisteelle tallennettavien tietojen muokkaus taas onnistuu yksinkertaisia tunnisteita käyttämällä keneltä tahansa, sillä niiden muokkausta ei useinkaan pysty estämään. ISO 15693 tunnisteita käyttämällä kirjoitetut tiedot voidaan kyllä suojata, mutta tämän jälkeen kukaan, ei edes alkuperäisten tietojen kirjoittaja, pysty niitä muokkaamaan.

Kehittyneemmät tunnisteet, kuten osa Mifare tunnisteista [22], mahdollistavat tiedon suojaamisen niin lukemisen kuin muokkaamisenkin varalta. Tällaisten tunnisteiden sisältämät tiedot ovat suojassa asiattomilta lukemisilta ja muokkaamisilta.

5.2.1 Suojattu tiedonsiirto

Suojattua tiedonsiirtoa käytettäessä on ensin tunnistettava toinen osapuoli ja vasta sen jälkeen voidaan aloittaa tiedonsiirto, jonka senkin tulee olla salattu. Tunnistamiseen ja salaamiseen käytetään avaimia. Avain voi olla joko symmetrinen tai epäsymmetrinen.

Symmetrisessä salausmenetelmässä sekä lukija että tunniste tuntevat saman avaimen, ja käyttävät tätä avainta tunnistaakseen toisen osapuolen. Avainta ei koskaan lähetetä siirtotien ylitse, vaan sitä käytetään salaamaan satunnaislukuja. Näin varmistetaan, että toinen osapuoli tuntee saman avaimen.

Kun tunniste saapuu lukijan lukuetäisyydelle, on niiden kummankin varmistuttava, että toinen osapuoli kuuluu samaan järjestelmään ja näin ollen voivat siirtää tietoa toisilleen. Ensimmäiseksi lukija lähettää tunnisteelle haasteen. Tunniste luo satunnaisluvun R_A ja lähettää sen lukijalle. Lukija luo toisen satunnaisluvun R_B ja salaa molemmat näistä numeroista avaimellaan sekä lähettää ne tunnisteelle. Tunniste purkaa näiden lukujen salauksen ja vertaa lukua R_A alkuperäiseen, luomaansa satunnaislukuun. Mikäli luvut ovat samat, tunniste on varmistunut lukijan identiteetistä. Tunniste lähettää vielä viestistä purkamansa luvun R_B lukulaitteelle minkä jälkeen lukulaite vertaa sitä alkuperäiseen lukuun R_B. Mikäli luvut ovat samat, lukulaite on varmistunut että tunniste tuntee saman avaimen ja näin ollen kuuluu samaan järjestelmään.[1]

Symmetrisen salauksen ongelmana on, että molempien osapuolten on tunnettava sama avain. Julkisissa järjestelmissä, joissa tunnisteiden määrä on suuri ja ne ovat kaikkien saatavilla, on olemassa pieni mahdollisuus, että avain pystytään selvittämään ja joutuessaan vääriin käsiin, sitä voidaan hyödyntää järjestelmää vastaan. Yksi tapa välttää tämä riski on käyttää järjestelmää, jossa jokaisella tunnisteella on oma avaimensa. Tällöin tunnisteen avain luodaan sen sarjanumeron perusteella käyttäen luonnissa lukulaitteen tiedossa olevaa salaista avainta. Tässä tapauksessa tunnisteen saapuu lukulaitteen lähelle, lukulaite kysyy ensimmäisenä tunnisteen sarjanumeroa. Lukulaite laskee sitten sarjanumerosta salaisen avaimen avulla tunnisteen avaimen. Tämän jälkeen tunnistaminen tapahtuu aivan kuten symmetriselläkin järjestelmällä käyttäen tunnisteen avainta. Ainoana erona on siis se, että lukulaite ei tiedä tunnisteen avainta ennen kun se on laskenut sen tunnisteen sarjanumeron perusteella.[1]

5.2.2 Salattu tiedonsiirto

Kun tiedonsiirron toinen osapuoli on tunnistettu, voidaan aloittaa tiedonsiirto. Vielä on kuitenkin mahdollista, että jokin kolmas osapuoli joko kuuntelee tiedonsiirtoa tai sekaantuu tiedonsiirtoon muokkaamalla sitä edukseen.

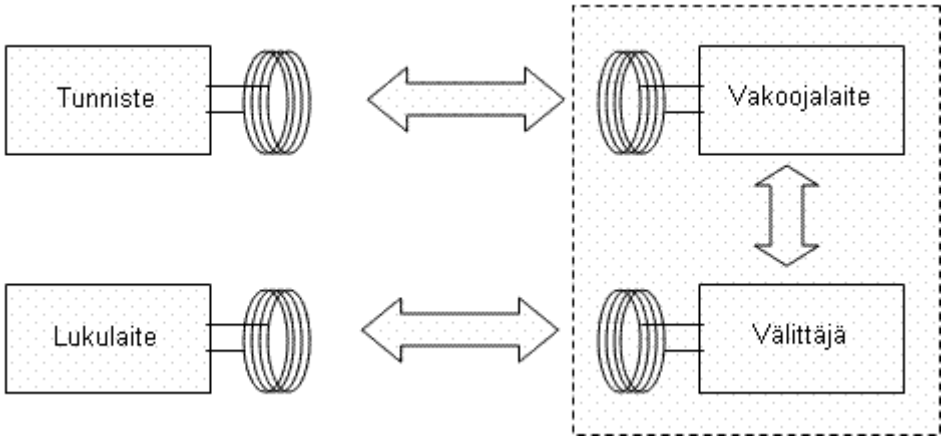
Kumpaakin näistä tapauksista vastaan voidaan suojautua salaamalla siirrettävä tieto ennen lähetystä, jolloin salakuuntelija ei ymmärrä kuulemaansa viestiä, eikä tiedon muokkaaja kykene muokkaamaan viestin sisältöä järkevästi niin ettei muutos paljastu. Salauksessa tieto salataan lähettävässä päässä ennen tiedon siirtoa siirtotien yli, ja salaus puretaan vastaanottopäässä. Salaukseen voidaan käyttää joko kummassakin päässä samaa avainta, jolloin kyseessä on symmetrinen järjestelmä, tai eri avainta jolloin kyseessä on asymmetrinen järjestelmä. Salausjärjestelmä voi olla joko jonosalausjärjestelmä, jossa jokainen merkki salataan erikseen, tai lohkosalausjärjestelmä, jossa tieto salataan lohkoissa. RFID–järjestelmissä käytetään lähinnä symmetrisiä jonosalaimia [1].

5.2.3 Tunnisteen kopiointi

Mikäli tunnisteen ja lukulaitteen välistä tiedonsiirtoa ei ole millään tavalla salattu, voi kuka tahansa salakuunnella sitä, ja kun tunnisteen sarjanumero on saatu luettua, voidaan sitä käyttää identiteetin väärentämiseen. Jonathan Westhues on esittänyt, kuinka tunnisteen lähettämä sarjanumero voidaan ensin lukea ja sen jälkeen toistaa samalla laitteella toiselle lukulaitteelle [17][18]. Näin toinen, huijattavaan järjestelmään kuuluva lukulaite kuvittelee alkuperäisen tunnisteen olevan läheisyydessään. Jotta identiteetin väärentäminen onnistuu, on lukulaite ensin saatava kopioitavan tunnisteen läheisyyteen. Näin sen sarjanumero saadaan luettua ja talletettua muistiin. Seuraavaksi sarjanumeron lukenut laite vaihdetaan tilaan, jossa se ei enää toimi lukulaitteena, vaan esiintyy tunnisteena lähettäen lukemaansa sarjanumeroa. Nyt laitteen kanssa mennään ”oikean” lukulaitteen luokse ja annetaan sen lukea kopioitu sarjanumero. Lukulaite ei huomaa eroa tämän kopiointiin käytettävän laitteen ja alkuperäisen tunnisteen välillä, vaan kuvittelee lukevansa alkuperäisen tunnisteen ja toimii sen mukaisesti.

Mikäli sekä tunniste että lukulaite varmistavat toistensa identiteetin ennen tiedonsiirron aloittamista, ei edellä kuvattu toimintatapa toimi, sillä tunnisteen lukeminen ei onnistu järjestelmään kuulumattomalla lukulaitteella. Tällöin on kuitenkin mahdollista käyttää luvattomasti lukulaitteen toimintaetäisyyden ulkopuolella sijaitsevaa tunnistetta linkittämällä tunniste ja lukulaite yhteen kuten Ziv Kfir ja Avishai Wool [23] sekä Gerhard Hancke [24] ovat osoittaneet. Molemmissa julkaisuissa käytettiin ISO 14443 standardin mukaisia tunnisteita ja lukulaitteita. Hyökkäyksen toteuttamiseen tarvitaan vakoojalaite joka esiintyy

lukulaitteena tunnisteelle ja välittäjälaite joka esiintyy tunnisteena lukulaitteelle sekä tiedonsiirtoyhteys näiden välille. Järjestelmään kuuluvien lukulaitteen ja tunnisteen välille luodaan siis keinotekoisesti yhteys kopioimalla kummankin lähettämät tiedot ja lähettämällä ne vastaanottajalle. Järjestelmän rakenne näkyy kuvassa 18.



Kuva 18. Identiteetin varastamiseen käytettävän järjestelmän rakenne

Näin toimittaessa ei saada selville tunnisteen todellista sarjanumeroa, eikä varastettua identiteettiä voida käyttää muulloin kuin varastamishetkellä. Eli kun tunnisteen identiteetti halutaan varastaa, tarvitaan identiteetin varastava lukulaite tunnisteen läheisyyteen ja tunnisteen lähettämän signaalin toistava laite lukulaitteen läheisyyteen, sekä yhteys näiden välillä. Laitteiden välisen tiedonsiirtoyhteyden on oltava riittävän nopea, jotta ne ehtivät vastata tunnisteen ja lukulaitteen lähettämiin signaaleihin ennen kuin protokolla tulkitsee yhteyden katkenneen.

5.2.4 RFID-järjestelmän tietoturva

RFID-järjestelmiä vastaan voidaan hyökätä samoin kuin mihin tahansa julkisessa verkossa sijaitsevaa palvelua vastaan. RFID-tunnisteita voidaan itsessään käyttää näissä hyökkäyksissä vaikkakin ne ovat resursseiltaan rajallisia. Tunnisteita voidaan käyttää hyökkäyksiin seuraavilla kolmella tavalla [8]:

1. Puskurin ylivuoto

    - Puskurin ylivuoto voi tapahtua käytettäessä ohjelmointikieliä, jotka eivät ole ”muisti-turvallisia” kuten C tai C++. Käsiteltäessä taulukkoa funktiolla, joka ei osaa havaita sen rajoja oikein, saadaan helposti aikaan puskurin ylivuoto. Tällöin voidaan erehdyksessä kirjoittaa tietoa puskurin ulkopuolelle ja näin sotkea muita ohjelman käyttämiä tietoja tai sen omaa ohjelmakoodia. Näin ohjelma ei enää toimi oikein.

2. Koodin lisäys

    - Vahingollista koodia voidaan lisätä syötteeseen niin, että jokin syötettä käsittelevä ohjelma ajaa sen. Tähän voidaan käyttää jotakin ohjelmointikieltä kuten VBScriptia tai Javascriptia. Tämä koodi voidaan ajaa epähuomiossa joko palvelimella tai mahdollisesti selaimessa kun tietokantaan syötettyjä tietoja käsitellään.

3. SQL-koodin syöttö

    - Yleensä RFID-järjestelmät käyttävät tietokantaa tietojen tallentamiseen. Tällöin tietoja haetaan, lisätään ja muokataan käyttäen SQL–kieltä (Structured Query Language). Tämä mahdollistaa myös sen, että hyökkääjä voi käyttää RFID-tunnisteeseen kirjoitettuja SQL-komentoja hyökkäyksessään järjestelmää vastaan. Tämä voi tapahtua esimerkiksi seuraavasti: Kun RFID-tunniste luetaan, järjestelmän on tarkoitus lisätä sen sisältämät tiedot tietokantaan. Tunnisteeseen on kuitenkin kirjoitettujärjestelmän odottamien tietojen sijaan SQL–komentoja, jotka katkaisevat lisäyskäskyn ja sisältävät sen jälkeen muita käskyjä joilla on tarkoitus sotkea tietokannan toimintaa.

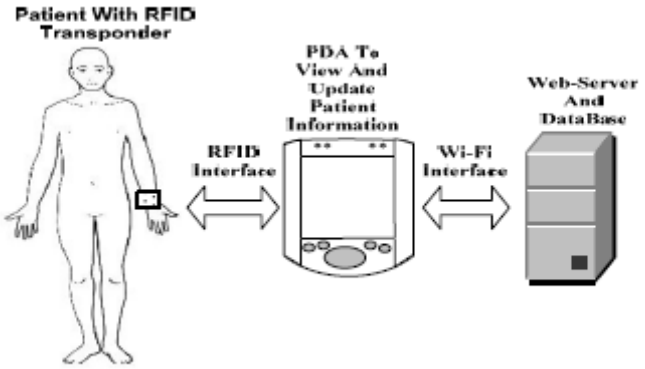
RFID-järjestelmää suunniteltaessa on siis varauduttava tietoturvan näkökulmasta samoihin asioihin kuin muidenkin tietojärjestelmien tapauksessa. RFID-tunnisteiden tietosisältöön ei voida luottaa, vaan niitä voidaan käyttää haitallisen tiedon syöttöön kuten mitä tahansa muuta tietoyhteyttä.

6. RFID-JÄRJESTELMÄ

Kun puhutaan RFID-järjestelmästä, tarkoitetaan kaikkia laitteita ja ohjelmistoja, joilla tunnisteita sekä tunnisteiden sisältämiä ja niihin liittyviä tietoja käsitellään. Toimiakseen RFID-järjestelmä vaatii vähintään seuraavat komponentit:

1. Tunniste
2. Lukulaite
3. Lukulaitetta käyttävä tietokone tai muu laite ohjelmistoineen

Tällainen järjestelmä saattaa olla riittävä, mikäli tunnisteisiin yhdistettävät tiedot kirjoitetaan suoraan niiden muistiin ja näitä tietoja ei tarvita muulloin kuin tunnistetta luettaessa. Usein tällainen järjestelmä ei kuitenkaan ole riittävä, vaan tietoja halutaan tallentaa myös muualle kuin itse tunnisteisiin. Tällöin tarvitaan jonkinlainen tietokanta tietojen tallentamista ja hakemista varten. Tällainen järjestelmärakenne esitettiin julkaisussa [11]. Tätä esimerkkijärjestelmää käytettiin potilaiden tunnistamiseen sairaalassa, ja tietokanta piti sisällään niin potilaan henkilötiedot kuin potilaan lääketieteelliset tiedotkin. Järjestelmän komponentit nähdään kuvassa 19.



Kuva 19. Järjestelmä potilaiden tunnistamiseksi [11]

Tässä järjestelmässä tietokannan tietojen käsitteleminen tapahtui selaimen avulla. Käyttöliittymä on toteutettu PHP-ohjelmointikielellä joka käsittelee MySQL-tietokantaan talletettuja potilastietoja. Tällaisen järjestelmän toteuttaminen on yksinkertaista ja vaatii ainoastaan seuraavat osat:

1. WWW-palvelinohjelmisto

2. Tietokantapalvelin

WWW-palvelinohjelmalla on oltava mahdollista ajaa omia ohjelmia, joiden avulla luodaan tapauskohtaisia, dynaamisia www-sivuja. Dynaamisesti luotavia sivuja voidaan käyttää tietokannan tietojen hakemiseen, muokkaamiseen ja lisäämiseen.

6.1 WWW-palvelimen toiminta

WWW-sivujen käyttämiseen tarvitaan selainohjelma ja palvelinohjelma. Selain ottaa yhteyden palvelimeen ja pyytää siltä tarvitsemaansa dokumenttia. Tyypillisesti dokumentti on HTML–kuvauskielellä toteutettu www-sivu, mutta se voi olla mikä tahansa muukin dokumentti, kuten kuva tai tekstitiedosto. Toiminta tapahtuu pyyntö/vastaus–parien mukaisesti. Selain lähettää ensin pyynnöt, johon palvelin sitten vastaa. Pyynnöt ja vastaukset toteutetaan http–protokollan mukaisesti.

Alla tyypillinen toimintatapaus:

1. Selain luo yhteyden palvelimeen (IP-osoite/portti) ja lähettää pyynnön haluamastaan dokumentista
2. Palvelin vastaanottaa pyynnöt ja tarkistaa onko kyseinen dokumentti saatavilla levyjärjestelmältä
    a. Jos on, palvelin lähettää OK viestin ja dokumentin
    b. Jos ei, palvelin lähettää vastauksena virhekoodin
3. Selain vastaanottaa tuloksen ja esittää sen käyttäjälle. Tulos voi olla pyydetty dokumentti tai virhekoodi

Selain voi, yllä kuvatun staattisen tiedon lisäksi, osata hallita dynaamista sisältöä joka siis luodaan kulloisenkin tilanteen mukaan ennen lähettämistä selaimelle. Tällaisen tiedon luomiseksi on olemassa useita eri tapoja kuten CGI- tai PHP–ohjelmat. Tällöin selain ei voi suoraan palauttaa pyydettyä dokumenttia, vaan sen sisältämä koodi täytyy ensin suorittaa. Palvelin kutsuu koodin suorittamiseen soveltuvaa ohjelmaa, joka ajaa koodin ja palauttaa tuloksen palvelimelle. Tämän jälkeen palvelin lähettää juuri luodun dokumentin selaimelle.

6.2 Esimerkkejä RFID-järjestelmistä

RFID-tekniikka on vielä suhteellisen uutta ja sen käyttö ei ole vielä vakiintunut yritysten toimintatapoihin. Yritykset ovat kuitenkin kiinnostuneita tekniikan suomista mahdollisuuksista ja joissakin käyttökohteissa RFID-tekniikka on jo käytössä. Seuraavaksi esittelen muutamia RFID-tekniikan sovelluksia. Esimerkeistä selviää kuinka RFID-tekniikkaa on käytetty logistiikan hallinnassa, tuotteiden alkuperän varmentamisessa, ihmisten havaitsemisessa ja ihmisten tunnistamisessa.

6.2.1 Wal-Mart ja RFID

Yhdysvaltalainen tavarataloketju Wal-Mart oli ensimmäisiä suuria RFID–tekniikan hyödyntäjiä. Kesäkuussa 2003 sata sen suurinta tavarantoimittajaa varustivat Wal-Martin Texasin jakelukeskukseen toimittamansa lavat ja laatikot RFID–tunnisteilla. Wal-Martilla oli tarkoitus RFID-tekniikkaa käyttämällä vähentää tilanteita joissa tuotteet ovat päässeet loppumaan kaupan hyllyiltä. Tuotteiden loppuminen hyllyiltä on merkittävä tekijä vähittäiskaupassa, Yhdysvalloissa noin 8 prosenttia myytävistä tuotteista on loppu hyllystä millä tahansa ajanhetkellä. Vaikka tämä luku ei suoraan vaikutakaan myyntilukuihin, on tyhjien hyllyjen arvioitu olevan 3.4 % jälleenmyyjille ja 2.6 % tavaran toimittajille.

Perinteisesti myymälän työntekijät ovat kierrelleet käytävillään ja huomatessaan, että jokin tuote on loppunut tai loppumassa, ovat he ilmoittaneet tilanteesta hyllyjen täyttäjille. Tässä ilmoittamisessa käytetään listoja, joilta hyllyihin toimitettavat tuotteet löytyvät.

Wal-Martilla tuotteet saapuvat myymälän hyllyille seuraavasti: Tuote saapuu toimittajalta Wal-Martin jakelukeskukseen, jakelukeskuksesta se toimitetaan myymälän varastotiloihin, josta se lopulta siirretään myymälän hyllyille kuluttajien saataville. Tässä toimitusketjussa RFID–teknologiaa hyödynnetään jakelukeskukseen saapumisen ja myymälän hyllylle siirtämisen välillä. Tuotteen lavaan kiinnitetty RFID–tunniste luetaan ensimmäisen kerran sen kulkiessa jakelukeskuksen portista sisään. Tuotteet viipyvät jakelukeskuksessa ennalta määräämättömän ajan, jonka jälkeen lavat puretaan ja laatikot lajitellaan ja lopulta lähetetään myymälään. Laatikkojen RFID–tunnisteet luetaan lajittelun aikana ja lopulta niiden lähtiessä jakelukeskuksen portista ulos.

Tuotelaatikoiden saapuessa myymälään niiden tunnisteet luetaan jälleen laatikon kulkiessa portista sisään myymälän varastoon. Toinen lukupiste on myymälätiloihin johtava ovi. Varsinaisissa myymälätiloissa ei lukulaitteita käytetä. Laatikon tunnisteen viimeinen luku tapahtuu, kun tyhjä laatikko hävitetään.

Hyödyt RFID-tekniikan käytöstä tulevat siitä, että nyt tiedetään jatkuvasti niin myymälävarastojen kuin jakelukeskuksienkin varastojen tila, sekä se, mitä tuotteita ja miten paljon on viety myymälätiloihin. Kun tämä tieto yhdistetään kassoilta saataviin yksittäisten tuotteiden myyntitietoihin, voidaan jo ennalta tietää mitkä tuotteet ovat loppumasta hyllytä ilman että kukaan käy tarkistamassa tilannetta paikan päällä. Näin hyllyihin toimitettavien tavaroiden lista voidaan päivittää automaattisesti.

Järjestelmän vaikutusta tuotteiden loppumiseen hyllystä testattiin kahdessatoista myymälässä Dallasissa. Lisäksi samoja asioita mitattiin kahdessatoista kontrolliryhmään kuuluvassa liikkeessä, joissa siis RFID–tekniikkaa ei ollut käytössä. Tutkimus kesti 29 viikkoa ja tänä aikana käytiin joka päivä kaikki hyllyt läpi etsien loppuneita tuotteita. Tuloksista laskettiin viikoittainen loppuneiden tuotteiden keskiarvo ja tämän viikoittaisen keskiarvon muutosta seurattiin ja verrattiin tuloksiin ilman RFID–tekniikkaa. Tulokset olivat todella lupaavia, RFID–tekniikan käyttö hyllyihin toimitettavien tavaroiden listojen luonnissa vähensi tavaroiden loppumisia 26 prosenttia. RFID–tekniikan käyttö ei kuitenkaan selitä tätä tuloksen paranemista kokonaan vaan osa muutoksesta voi selittyä niin sanotulla *Hawtorne efektillä*, joka tarkoittaa sitä, että ihmiset muuttavat toimintaansa ollessaan tarkkailun alaisina ja näin ollen suoriutuvat tehtävistään erilailla. Tästä syystä tuotteiden loppumista hyllystä mitattiin myös kahdessatoista kontrolliryhmään kuuluvassa liikkeessä. Myös näissä liikkeissä tuotteiden loppumiset hyllystä vähenivät tutkimusjakson aikana, mutta muutos oli huomattavasti pienempi kuin RFID–tekniikkaa hyödyntävissä liikkeissä. Muutosnopeus RFID–tekniikkaa hyödyntävissä liikkeissä oli noin 63 prosenttia parempi kuin kontrolliryhmässä. Näin ollen RFID–tekniikan aikaansaaman parannuksen katsottiin olevan 26 % x 0.63 = 16 prosenttia.[5]

6.2.2 Pfizer ja RFID

Yhdysvaltalainen lääkevalmistaja Pfizer käyttää RFID–tekniikkaa vaikeuttamaan väärennettyjen lääkkeiden asemaa markkinoilla. Lääkkeiden väärennys on kasvava ongelma ja lääketeollisuus on selvittänyt erilaisia tekniikoita väärennösten kiinnisaamiseksi. Mikäli lääkepakkaukseen lisätään RFID–tunniste ja sen kulkemista toimitusketjussa seurataan tämän tunnisteen avulla, voidaan väärennösten ilmestymistä markkinoille vähentää merkittävästi. Järjestelmässä käytetään EPC–standardin mukaisia HF–taajuusalueen RFID–tunnisteita. Tehtaalla yksittäiseen lääkepakkaukseen lisätään EPC–tunniste ja tietokantaan merkitään, että tämä tunniste on otettu käyttöön. Lääkepakkauksen tunniste luetaan sen lähtiessä tehtaalta ja tämä myös merkitään tuotteen tietoihin tietokantaan. Samalla tavalla näitä lukutapahtumia ja merkintöjä tietokantaan kertyy eri vaiheessa toimitusketjua ja näin tietokannasta voidaan seurata yksittäisen lääkepakkauksen matka tehtaalta apteekkiin. Nyt mikäli väärennettyjä

tuotteita pyrkii markkinoille ja niissä ei ole sopivaa RFID–tunnistetta, huomataan väärennös heti kun pakkauksen tunnistetta yritetään lukea. Vaikka väärennettyyn pakkaukseen olisi lisätty sopiva RFID–tunniste, huomataan väärennös siinä vaiheessa kun tietokannasta haetaan tuotteen tiedot ja huomataan, että tämä kyseistä tunnistetta ei löydy koko tietokannasta. Vielä on mahdollista että väärennetyssä tunnisteessa on sellainen EPC–koodi joka todellakin löytyy tietokannasta. Tässä tapauksessa tietokannasta voidaan huomata, että sama tuote on vaikkapa merkitty saapuneeksi kahteen eri apteekkiin. Tällöin tiedetään se, että toinen näistä tuotteista on väärennös ja asia voidaan selvittää.[6][7]

Tällä hetkellä RFID–tunnisteiden korkea hinta estää niiden laajemman käyttöönoton yksittäisten pakkausten seurannassa. Pfizer esimerkiksi on ottanut tunnisteet tässä vaiheessa käyttöön ainoastaan Viagra–lääkkeessä, joka onkin yrityksen eniten väärennetty tuote.

6.2.3 RFID kaivosteollisuudessa

Turvallisuus on tärkeä tekijä kaivosteollisuudessa. Törmäyksiä ihmisten ja kaivoskoneiden välillä tapahtuu vaatien usein ihmishenkiä. Näiden onnettomuuksien välttämiseksi on kokeiltu useita eri tekniikoita kuten tutkaa, videokameroita, ultraääntä ja infrapunaa ja viimeisimpänä RFID-tunnistusta [14]. Tässä käyttötarkoituksessa ei tarvita RFID-tunnisteiden muistiominaisuuksia vaan ainoastaan tieto siitä, onko koneen läheisyydessä tunnisteita. Järjestelmä ei siis kerro, kuka koneen läheisyydessä on, vaan ainoastaan sen, onko koneen läheisyydessä ihminen tai ihmisiä. Järjestelmä koostuu työkoneisiin kiinnitetyistä lukulaitteista ja työntekijöiden kypärään kiinnitetyistä tunnisteista. Työkoneiden lukulaitteissa on useita antenneja suunnattuna eri suuntiin, jotta se huomaisi tunnisteet eri puolilla konetta.

Toimiakseen luotettavasti järjestelmän on kyettävä havaitsemaan kaikki tunnisteet noin 15 metrin etäisyydeltä. Testeissä käytettiin passiivisia LF-tunnisteita ja aktiivisia UHF-tunnisteita. LF-tunnisteiden ongelma oli aivan liian lyhyt lukuetäisyys (vain noin kaksi metriä). UHF-tunnisteiden ongelma oli vaihtelevat lukuetäisyydet riippuen esteistä lukulaitteen ja tunnisteen välillä ja tunnisteen asennosta. Mikäli työntekijän vartalo oli tunnisteen ja lukulaitteen välillä, tippui lukuetäisyys huomattavasti. Samoin jos tunniste ei ollut suunnitellussa asennossa vaikkapa silloin, kun työntekijä oli kumartuneena, oli lukuetäisyys huomattavasti normaalia heikompi. Vaihtelevat lukuetäisyydet aiheuttavat vääriä hälytyksiä, kun tunniste luetaankin todella kaukaa ja liian myöhäisiä hälytyksiä, kun tunnisteen havaitseminen tapahtuu vasta aivan koneen läheisyydessä.

Loppupäätelmänä RFID-tekniikkaa pidettiin lupaavana, mutta jatkokehitystä tarvitaan jotta työntekijät voitaisiin havaita sen avulla luotettavasti kaivoksissa.

6.2.4 RFID passeissa

Suomi alkoi myöntää uusia niin sanottuja biopasseja 21.8.2006 [25]. Biopassi eroaa vanhan mallisesta passista sillä, että se sisältää RFID-tunnisteen, johon on tallennettu passin omistajan valokuva ja samat henkilötiedot, jotka löytyvät passista muutenkin. Tämän lisäksi tunnisteeseen on myöhemmin tarkoitus tallentaa passin omistajan sormenjälkitiedot. Tunnisteeseen tallennetut tiedot on suojattu digitaalisella allekirjoituksella [26]. Tämän julkiseen avaimeen perustuvan järjestelmän avulla voidaan varmistua siitä, että passin on myöntänyt siihen oikeutettu taho ja ettei tunnisteen tietoja ole myöntämisen jälkeen muokattu. Näin passin väärentäminen vaikeutuu huomattavasti.

RFID-tunnisteen käyttö on herättänyt epäilyksiä, että passia voitaisiin käyttää ihmisten luvattomaan seurantaan. Kriitikot pelkäävät, että kuka tahansa voi lukea passin omistajan henkilötiedot kenenkään huomaamatta. Tästä syystä passin suunnittelussa on kehitetty varokeinoja luvattoman lukemisen estämiseksi.

Tunnisteen luvaton lukeminen on estetty ensinnäkin sillä, että passin kannet sisältävät metallikerroksen, joka muodostaa Faradayn häkin ja estää tunnisteen lukemisen kun passi on suljettuna [20]. Tunnisteen lukeminen vaatii myös koodin, joka on tulostettu passin pintaan. Tunniste ei lähetä mitään tietoja ilman tätä koodia. Näin ollen tunnisteen tietojen lukeminen vaatii aina näköyhteyden passiin ja sen että passi on avoinna. Passin tietoja ei siis pystytä lukemaan esimerkiksi laukun sisällä tai taskussa olevasta passista.

7. TESTIT JA TOTEUTETTU JÄRJESTELMÄ

Tämä työ on tehty osana EtapII projektia, jossa oli tarkoitus selvittää tekniikat, joiden avulla voidaan tunnistaa betonista valmistetut elementit elementtituotannon aikana, rakennuspaikalla ja valmiissa rakennuksessa koko elementin elinkaaren ajan sekä siirtämään elementtiin liittyvät mitta- ja muut tiedot tälle paikalle.

Tavoitteena oli siis yksittäisten elementien luotettava ja nopea tunnistaminen rakennustuotannon eri vaiheissa. Elementtien tunnistamisella on useita suotuisia vaikutuksia. Ensinnäkin vaikutuksena on virheiden vähentäminen. Kun elementti pystytään luotettavasti tunnistamaan, voidaan tuotannon eri vaiheissa välttää virheitä, kun tiedetään, mikä elementti on kyseessä. Näin voidaan varmistua esimerkiksi siitä että elementtiä käsitellään oikealla tavalla, se kuljetetaan oikeaan paikkaan ja asennetaan oikeaan kohtaan rakennusta.

Toisnen syy työn tekemiseen liittyy aikaisempaan tutkimukseen jossa kehitettiin laitteisto jolla elementin toteutuneet mitat voidaan elementtivalmistuksen jälkeen mitata tarkasti. Laadunvarmistuksen lisäksi tätä mittatietoa on mahdollista hyödyntää rakennuspaikalla elementtiä paikalleen asennettaessa. Elementin mitoissa sallitaan pienet heitot suunnitelluista mitoista ja elementti voidaan asentaa paikalleen, kunhan mitat ovat toleranssien sisällä. Kuitenkin elementin todellisia mittoja voidaan hyödyntää sitä paikalleen asennettaessa. Toteutuneet mitat voidaan ottaa huomioon asennuksessa ja näin ollen todellisten ja suunniteltujen mittojen eron vaikutus lopputulokseen pienenee.

Elementtien tunnistamisesta on hyötyä myös virhetilanteisiin johtavien syiden selvittämisessä. Kun elementit voidaan luotettavasti tunnistaa vielä vuosienkin jälkeen valmistamisesta, voidaan paremmin selvittää syyt, jotka johtavat mahdollisiin puutteisiin laadussa. Kun viallinen elementti tunnistetaan, voidaan siihen liitettyjen tietojen avulla etsiä syitä kyseiseen vikaan. Näin voidaan esimerkiksi löytää yhdistäviä tekijöitä eri viallisten elementtien välillä, kuten sama betonierä. Näitä löydettyjä tietoja voidaan käyttää tulevaisuudessa laadun parantamiseen.

Laadun parantamisen lisäksi jäljitettävyys auttaa vastuullisen osapuolen selvittämisessä virhetapauksessa. Kun elementti voidaan jälkikäteen tunnistaa, voidaan myös varmistua, että se on asennettu oikeaan paikkaan. Samoin erimielisyydet elementin mitoista voidaan tarkistaa tietokannasta, mikäli elementti mitataan valmistuksen jälkeen. Näin voidaan varmistua siitä, ovatko jo paikalleen asennetun elementin mitat toleranssien rajoissa, ja voidaan selvittää johtuuko ongelmat elementin paikalleen asentamisessa virheellisistä elementin mitoista vai virheellisestä asennuksesta.

Projektin tavoitteet pystytään toteuttamaan hyödyntäen RFID–tekniikkaa. Elementtiin upotetaan valmistuksen yhteydessä RFID –tunniste joka sisältää yksilöllisen sarjanumeron. Tämän sarjanumeron avulla tunniste ja samalla elementti, johon se on sijoitettu, yhdistetään tietokannassa tämän kyseisen elementin tietoihin.

Tunnisteen sisältämät tiedot luetaan lukulaitteella, joka lukee tunnisteen tiedot ja lähettää ne tietokoneelle. Tietokone ottaa yhteyden tietokantaan ja tunnisteen sarjanumeron avulla hakee elementin tiedot, jotka esitetään käyttäjälle. Käyttäjä voi nyt tietojen tarkistamisen lisäksi listätä uusia tietoja tai muokata olemassa olevia tietoja.

7.1 Testit

Testien tarkoituksena oli selvittää soveltuuko RFID-tekniikka ylipäätään tietojen siirtämiseen rakennuspaikalle ja mikäli soveltuu, selvittää minkälaiset laitteet olisivat parhaita mahdollisia ja mitkä ovat niiden ominaisuudet. Testit suoritettiin kolmessa eri vaiheessa. Ensin järjestettiin esitestit, joiden avulla kartoitettiin, minkälaisia RFID-tuotteita eri toimittajilla oli tarjolla tähän käyttötarkoitukseen. Seuraavan vaiheen muodostivat omat lukutestit, joissa esitestien perusteella valittuja laitteita testattiin tarkemmin eri olosuhteissa. Tässä vaiheessa tunnisteiden sisältämien tietojen lukemista testattiin esimerkiksi erilaisten väliaineiden läpi, jotta niiden vaikutukset lukutapahtumaan saatiin selville. Lopuksi laitteita testattiin käytännössä yhden rakennuskohteen elementtien kanssa. Tässä vaiheessa toteutettiin myös elementtien tietojen tallentamiseen, käsittelyyn ja hakuun soveltuva tietojärjestelmä, jota hyödyntämällä elementtien tietojen käsittely onnistuu sijainnista riippumatta.

7.1.1 Esitestit

Esitestien tarkoituksena oli kartoittaa erilaisten lukulaitteiden ja tunnisteiden toimivuus betoniin upotettuna. Testiin osallistui laitteita kolmelta laitetoimittajalta. Testattavaksi saatiin niin HF- kuin UHF–taajuusalueita käyttäviä tunnisteita sekä niiden tietojen lukemiseen soveltuvia lukulaitteita.

Testejä varten valettiin erillisiä testielementtejä, joiden betonin sekaan upotettiin tunnisteita. Testilementti nähdään kuvassa 20. Testielementit suunniteltiin sellaisiksi, että ne vastaavat mahdollisimman hyvin todellisia elementtejä. Tunnisteita upotettiin ensinnäkin aivan pinnan lähelle, noin *senttimetrin* syvyyteen, toiseksi *80 mm* syvyyteen, niin että päällä on pelkkää betonia ja kolmanneksi *80 mm* syvyyteen niin, että tunnisteen päällä menee myös raudoitus (tunniste ei kuitenkaan kokonaan raudan alla).

Kuva 20. Esitesteissä käytetty elementti

Testeihin ei valitettavasti saatu UHF-taajuusalueen käsilukijaa vaan ainoastaan suurempia, kiinteään asennukseen tarkoitettuja lukulaitteita. Testeissä kuitenkin nähtiin, kuinka tunnisteen upottaminen betoniin muuttaa UHF-tunnisteen viritystaajuutta, eli taajuutta, johon se reagoi ja näin ollen sen lukeminen hankaloituu. Tämä ongelma olisi mahdollista kiertää ainakin osittain suunnittelemalla tunniste nimenomaan tätä tarkoitusta varten, jolloin sen viritystaajuus olisi betoniin upotettuna mahdollisimman lähellä oikeaa, lukulaitteen lähettämää taajuutta. Parhaimmillaan betoniin upotettu UHF-tunniste löydettiin noin kahden metrin etäisyydeltä, mutta pienimmillään etäisyys oli vain noin kymmenen senttimetriä. Näissä testeissä oli siis käytössä suuri, kiinteään asennukseen tarkoitettu antenni, joka kykenee lukemaan tunnisteen sisältämät tiedot noin viiden metrin päästä, kun välissä on pelkkää ilmaa.

HF-taajuusalueen tunnisteita ja lukulaitteita oli testeissä kahdelta eri valmistajalta. HF-tunnisteiden lukuetäisyydet eivät kiinteälläkään lukijalla yllä kovin pitkälle, ja käsilukijalla lukuetäisyydet jäivät viiden ja kymmenen sentin väliin betonin pinnasta, kun tunniste oli upotettu noin sentin verran pinnan alle.

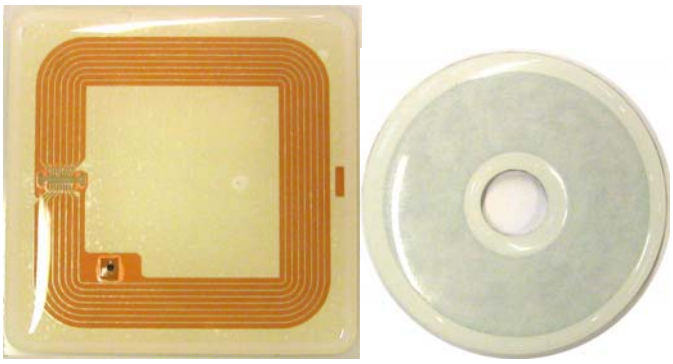
Esitestien perusteella jatkotesteihin valittiin kuvassa 21 näkyvä FEIG PRH100-lukulaite HF-tunnisteille ja ISO 15693 standardin mukaisia tunnisteita. Syynä HF-tekniikan valitsemiseen oli se, että se ei ole niin altis väliaineiden aiheuttamille häiriöille ja se, että sekä lukulaite että tunnisteet voitiin ottaa heti testikäyttöön eikä jatkokehittelyä tarvittu. UHF-taajuusalueen tunnisteiden valitseminen olisi edellyttänyt lisätutkimuksia jossa selvitetään betoniin upottamisen vaikutus tunnisteen viritystaajuuteen ja toisaalta olisi jouduttu odottamaan että käyttötarkoitukseemme soveltuvia kannettavia lukulaitteita olisi tullut markkinoille. HF-

taajuusalueen lukulaitteista PRH100 oli lukuetäisyydeltään selvästi parempi ja hinnaltaankin edullinen kilpailijaan verrattuna, joten se valittiin jatkotesteihin. Tämän lisäksi PRH100 oli ainoa testattu lukulaite joka kykeni lukemaan 80 mm syvyyteen upotettujen tunnisteiden sarjanumerot jopa niin, että tunnisteen ja lukulaitteen välissä kulki ohut raudoitus. Näin ollen PRH100 osoittautui parhaaksi vaihtoehdoksi jatkotesteihin.

Kuva 21. Testeissä käytetty FEIG PRH100-lukulaite

7.1.2 Omat lukutestit

Esitestien jälkeen testattavaksi saatiin FEIG PRH100-lukulaite HF-taajuusalueen tunnisteille. Lisäksi testattavana oli kahta ulkomuodoltaan erilaista ISO 15693-standardin mukaista tunnistetta. Toinen niistä on noin 45 mm halkaisijaltaan oleva pyöreä tunniste, jonka keskellä on reikä. Toinen taas on suurempi, noin 60*60 mm kokoinen neliskanttinen tunniste. Tunnisteet on nähtävissä kuvassa 22. Tunnisteet eroavat ainoastaan kokonsa ja muotonsa puolesta, toiminnaltaan ne ovat täysin identtisiä. Testeissä näitä tunnisteita ja lukulaitetta testattiin eri olosuhteissa, jotta niiden vaikutus lukutapahtumaan selviäisi. Tunnisteiden lukuetäisyys, kun väliaineena on ainoastaan ilma, eroaa varsin selvästi. Pienemmän pyöreän tunnisteen lukeminen onnistuu noin *kahdeksan senttimetrin* päästä, kun taas suuremman, neliön muotoisen, *jopa 16 senttimetrin* päästä.



Kuva 22. Testeissä käytetyt tunnisteet

Betoni vaikuttaa lukuetäisyyteen negatiivisesti. Lukeminen ei esty kokonaan, mutta lukuetäisyys tippuu hiukan. Kun nämä kaksi tunnistetta oli upotettu 40 mm syvyyteen betoniin muuttui niiden lukuetäisyys seuraavasti. Suuremman tunnisteen lukuetäisyys oli nyt 130 mm, josta 40 mm oli siis betonia ja loput 90 mm ilmaa. Pienemmän pyöreän tunnisteen lukuetäisyydeksi tuli 75 mm, josta 40 mm betonia ja 35 mm ilmaa. Kun tunnisteet upotettiin 65 mm syvyyteen, olivat lukuetäisyydet seuraavanlaisia. Suuremman tunnisteen lukuetäisyydeksi tuli 100 mm, eli 65 mm betonia ja 35 mm ilmaa. Pienemmän, pyöreän tunnisteen lukeminen ei tältä syvyydeltä enää onnistunut.

Seuraavaksi tunnisteiden lukemista testattiin niin, että tunnisteet upotettiin veteen. Tällöinkään lukeminen ei estynyt kokonaan, mutta lukuetäisyys tippui ilmaan verrattuna. Kun pyöreä tunniste upotettiin 40 mm syvyyteen veteen, sen lukeminen onnistui enää 25 mm päästä veden pinnasta eli kokonaisetäisyys lukulaitteen ja tunnisteen välillä oli 65 mm. Suuremmalla neliön muotoisella tunnisteella vastaavat etäisyydet olivat 70 mm veden pinnasta eli 110 mm kokonaisetäisyys.

Myös tunnisteiden toiminta jään sisällä testattiin. Aivan kuten muissakin testeissä tunnisteet upotettiin 40 mm syvyyteen jään sisälle ja lukuetäisyydet mitattiin. Pienemmällä pyöreällä tunnisteella lukuetäisyydeksi saatiin 35 mm jään pinnasta eli 75 mm etäisyys tunnisteen ja lukulaitteen välillä. Suuremmalla tunnisteella etäisyydeksi saatiin 110 mm jään pinnasta eli 150 mm kokonaisetäisyys.

Taulukko 6. Toteutuneita lukuetäisyyksiä eri väliaineissa

Tunniste	Ilma	40mm betoni	65mm betoni	40mm vesi	40mm jää
Pyöreä	80	75	-	65	75
Neliö	160	130	100	110	150

Taulukkoon 6 on kerätty lukuetäisyyksiä eri väliaineissa. Taulukossa esitetyt etäisyydet kuvaavat kokonaisetäisyyttä lukulaitteen ja tunnisteen välillä, eli etäisyys koostuu väliainesta ja ilmasta. Tunniste upotettiin väliaineeseen joko 40 tai 65 mm syvyyteen ja lukuetäisyys tunnisteeseen mitattiin. Taulukosta nähdään että lukuetäisyydet putoavat eniten kun tunniste on upotettuna veteen, jään ja kuivan betonin vaikutus on vähäisempi.

Taulukossa 6 lueteltujen väliaineiden lisäksi myös betonin kuivumisen vaikutus lukuetäisyyksiin testattiin. Testissä tunniste upotettiin 40 mm syvyyteen märkään betoniin ja maksimi lukuetäisyys mitattiin. Tämän jälkeen lukutesti uusittiin tunnin välein ja lukuetäisyys

mitattiin. Näiden testien perusteella tunnisteen lukeminen märästä betonista heti valun jälkeen onnistuu samalta etäisyydeltä kuin veden läpi eli tässä tapauksessa 110 mm kokonaisetäisyydeltä käytettäessä suurempaa, neliön muotoista tunnistetta. Betonin kuivuessa lukuetäisyys kasvaa ja jo noin kahden tunnin kuluessa se saavuttaa maksimiarvonsa eli suuremman, neliön muotoisen tunnisteen tapauksessa 130 mm etäisyyden.

Väliaineen lisäksi myös lukulaitteen ja tunnisteen asento toisiinsa nähden vaikuttavat lukuetäisyyteen. Lukuetäisyydet ovat suurimmillaan kun ne ovat toisiinsa nähden samansuuntaisesti, kulman muuttuessa lukuetäisyydetkin putoavat jopa nollaan käytettäessä pienikokoisia tunnisteita. Taulukkoon 7 on kerätty lukuetäisyyksiä eri kulmilla tunnisteen ja lukulaitteen välillä. Tunnisteena tässä testissä käytettiin neliön muotoista 60*60 mm kokoista tunnistetta, joka on nähtävissä kuvassa 22.

Taulukko 7. Kulman vaikutus lukuetäisyyksiin

Kulma	Lukuetäisyys (mm)
0°	158
15°	147
30°	135
45°	118
60°	110
75°	68
90°	24

7.2 Toteutettu järjestelmä

Projektin käytännön testeissä käytettävä järjestelmä koostuu betoniin upotettavasta tunnisteesta, lukulaitteesta ja palvelintietokoneesta, jolla elementtitietokanta sekä tietojen käsittelyn mahdollistavan käyttöliittymän toteuttava www-palvelin sijaitsevat. Järjestelmän rakenne on kuvattu kuvassa 23.

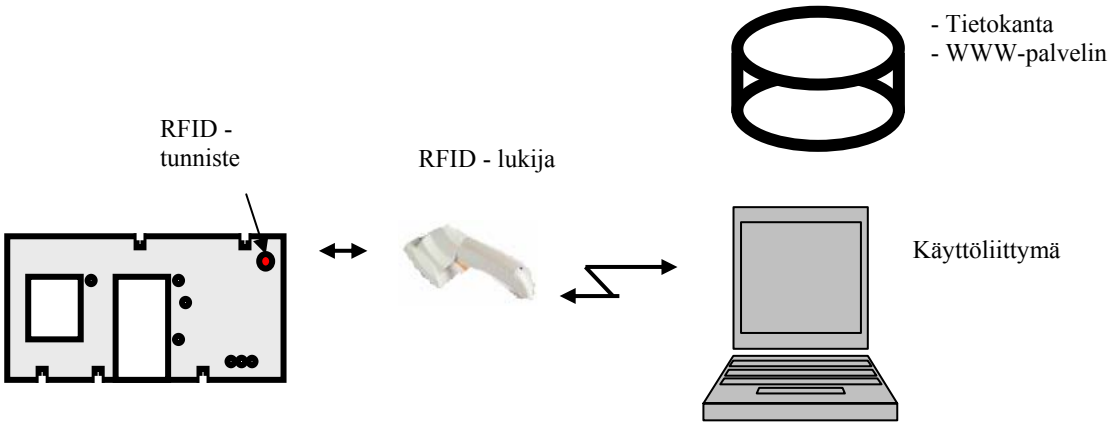
Tunnisteena päädyttiin käyttämään HF–taajuusalueen tunnistetta, koska ne osoittautuivat testeissä luotettavammiksi kuin korkeammalla UHF-taajuusalueella toimivat tunnisteet. HF-taajuusalueella tunnisteen virransaanti ja tiedonsiirto perustuu muuttuvaan magneettikenttään. Tämä ei tekniikkana ole niin herkkä väliaineen vaikutukselle kuin sähkömagneettista säteilyä hyödyntävä UHF–tekniikka. UHF–tunnisteiden viritystaajuus muuttuu kun ne ovat kosketuksissa toiseen aineeseen. Tämä voi aiheuttaa sen, että tunnisteen lukeminen betoniin upotettuna ei onnistu ollenkaan tai ainakin lukuetäisyydet tippuvat huomattavasti. Esitesteissä huomattiin, että UHF-taajuusalueen tunnisteiden lukuetäisyydet tippuivat huomattavasti, kun

ne upotettiin betoniin ja tunnisteiden lukeminen oli vaikeaa jopa suurilla, kiinteään asennukseen tarkoitetuilla antenneilla. HF–tekniikkaa käytettäessä signaali kyllä heikkenee väliaineessa, mutta tämä ei estä lukemista kokonaan, vaan se ainoastaan lyhentää lukuetäisyyttä jonkin verran.

HF–taajuusalueen käyttämisen huonona puolena ovat lyhyemmät lukuetäisyydet kuin UHF–taajuusalueella. UHF–alueen käyttämisellä jopa useiden metrien lukuetäisyydet ovat mahdollisia kiinteästi asennettavilla suuritehoisilla ja suurilla antennilla varustetuilla lukulaitteilla. Tämä mahdollistaisi erilaisten porttilukijoiden rakentamisen, joilla voidaan esimerkiksi tunnistaa kaikki tunnisteet, jotka kulkevat tehtaan ovesta ulos. HF–taajuusalueella tämä ei ole mahdollista, sillä tekniikan mahdollistama teoreettinen suurin lukuetäisyys on noin kolme metriä ja käytännössä kiinteästi asennettavia lukulaitteita käyttämällä päästään noin metrin lukuetäisyyksiin. Syynä HF–taajuusalueen huonompaan lukuetäisyyteen on se, että tiedon ja energian siirtämiseen käytetään muuttuvaa magneettikenttää. Magneettikenttä heikkenee etäännyttäessä sen lähteestä huomattavasti nopeammin kuin HF–tekniikassa käytetty sähkömagneettinen säteily.

Lukulaitteena toimii Saksalaisen Feig Electronicin valmistama PRH100 RFID–lukulaite. Tämä lukulaite ei toimi itsenäisenä tietojen käsittelijänä, vaan se vaatii parikseen tietokoneen tai jonkin muun vastaavan laitteen. Testeissä käytetty versio lukulaitteesta on kytketty tietokoneeseen USB-kaapelin avulla.

Palvelimella toimii tietokanta, joka pitää sisällään kunkin elementin tiedot sisältäen elementiin upotetut tunnisteen sarjanumeron, elementin tunnuskoodin, kohteen, johon elementti kuuluu, elementin mittatiedot ja elementin valmistuspäivämäärän. Tietokannasta voidaan hakea elementin tiedot elementtiin upotetun tunnisteen sarjanumeron perusteella.



Kuva 23. Testeissä käytetty järjestelmä

Testijärjestelmässä lukulaite on kytkettynä kannettavaan tietokoneeseen, jolla myös tietokanta ja käyttöliittymän toteuttava www-palvelin toimivat. Tällöin haut tietokannasta eivät kulje tietoverkon yli, vaan tiedon ainoastaan saman tietokoneen sisällä. Tuotantokäytössä kenttäolosuhteissa lukulaitteen parina voisi toimia Bluetoothilla varustettu puhelin, joka käyttää lukulaitetta tunnisteen sarjanumeron lukemiseen ja ottaa GPRS-tekniikalla yhteyden tehtaan palvelimeen, josta haetaan elementin tiedot tunnisteesta luetun sarjanumeron perusteella.

7.2.1 Järjestelmän toiminta

Järjestelmän käyttö alkaa elementin suunnittelutietojen lisäämisellä tietokantaan. Kun elementin valmistus alkaa, alkaa myös elementin seuranta RFID–tunnisteen avulla. Ennen kuin elementtiin upotetaan tunniste, sen sarjanumero luetaan lukulaitteella. Tämä sarjanumero täytyy lisätä tietokantaan oikean elementin tietoihin, jotta elementti voidaan myöhemmin tunnistaa. Kun tunnisteen sarjanumero on lisätty tietokantaan, voidaan tunniste upottaa elementtiin.

Tästä hetkestä eteenpäin elementti voidaan missä vaiheessa tahansa tunnistaa lukemalla siihen upotetun tunnisteen sarjanumero ja hakemalla tietokannasta sitä vastaavat tiedot.

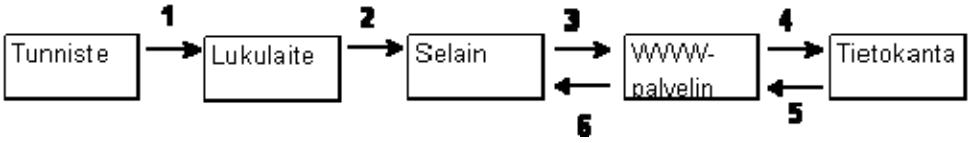
Lukulaite lukee tunnisteesta sarjanumeron ja lähettää sen tietokoneelle, johon se on kytkettynä ja joka hallitsee lukulaitetta. Tietokoneen selaimella on ennen tätä otettu yhteyttä www-palvelimeen, joka luo elementtien tietojen käsittelyssä tarvittavat www-sivut. Tietokone vastaanottaa sarjanumeron ja www-sivun käyttöliittymän avulla ottaa yhteyden tietokantaan, jossa elementtien tiedot sijaitsevat. Tietokannasta haetaan elementin tiedot tunnisteen sarjanumeron perusteella ja ne esitetään käyttäjälle.

7.2.2 Järjestelmän komponentit

Testijärjestelmä koostuu seuraavista komponenteista:

- RFID – tunnisteet
- Lukulaite
- Selain
- WWW-palvelin
- Tietokanta

ISO 15693-standardin mukaiset RFID-tunnisteet upotetaan elementin valmistuksen yhteydessä elementin sisään ennalta määrättyyn paikkaan. Lukulaitetta käytetään lukemaan tunnisteen sisältämä sarjanumero sekä siihen talletetut tiedot. Kun halutaan hakea elementin tietoja tietokannasta, siihen käytetään tarkoitukseen suunniteltua selaimella käytettävää käyttöliittymää. Tällöin lukulaite lähettää lukemansa tunnisteen sarjanumeron selaimella avatulle lomakkeelle. Tämän jälkeen selain pyytää WWW-palvelimelta uutta sivua, jolla elementin tiedot esitetään. Palvelin vastaanottaa pyynnöt ja lomakkeelle luetun sarjanumeron sekä alkaa käsitellä selaimen pyytämää sivua. Elementin tiedot sisältämä sivu luodaan dynaamisesti PHP–skriptikielen avulla. Palvelin tulkkaa ja suorittaa skriptin komennot. Komennot hakevat MySQL–tietokannasta kaikki kyseiseen tunnisteen sarjanumeroon liittyvät tiedot. Kun tiedot on haettu tietokannasta, luodaan niiden perusteella nämä tiedot esittävä WWW-sivu. Luotu sivu lähetetään takasin selaimelle, josta käyttäjä voi lukea hakemansa tiedot.



Kuva 24. Elementin tietojen hakemisen ja esittämisen eri vaiheet

Elementin tietojen hakeminen tietokannasta sen tunnisteen perusteella koostuu kuvassa 24 näkyvistä vaiheista.

1. Tunniste luetaan lukulaitteella
2. Lukulaite lähettää lukemansa sarjanumeron tietokoneella käynnissä olevalle selaimelle
3. Selain lähettää WWW-palvelimelle pyynnön uudesta sivusta
4. WWW-palvelin suorittaa sivun PHP -koodin, joka lähettää kyselyn tietokannalle
5. Tietokanta palauttaa oikean elementin tiedot WWW-palvelimelle
6. WWW-palvelin suorittaa PHP–koodin loppuun luoden uuden WWW–sivun ja lähettää sen selaimelle

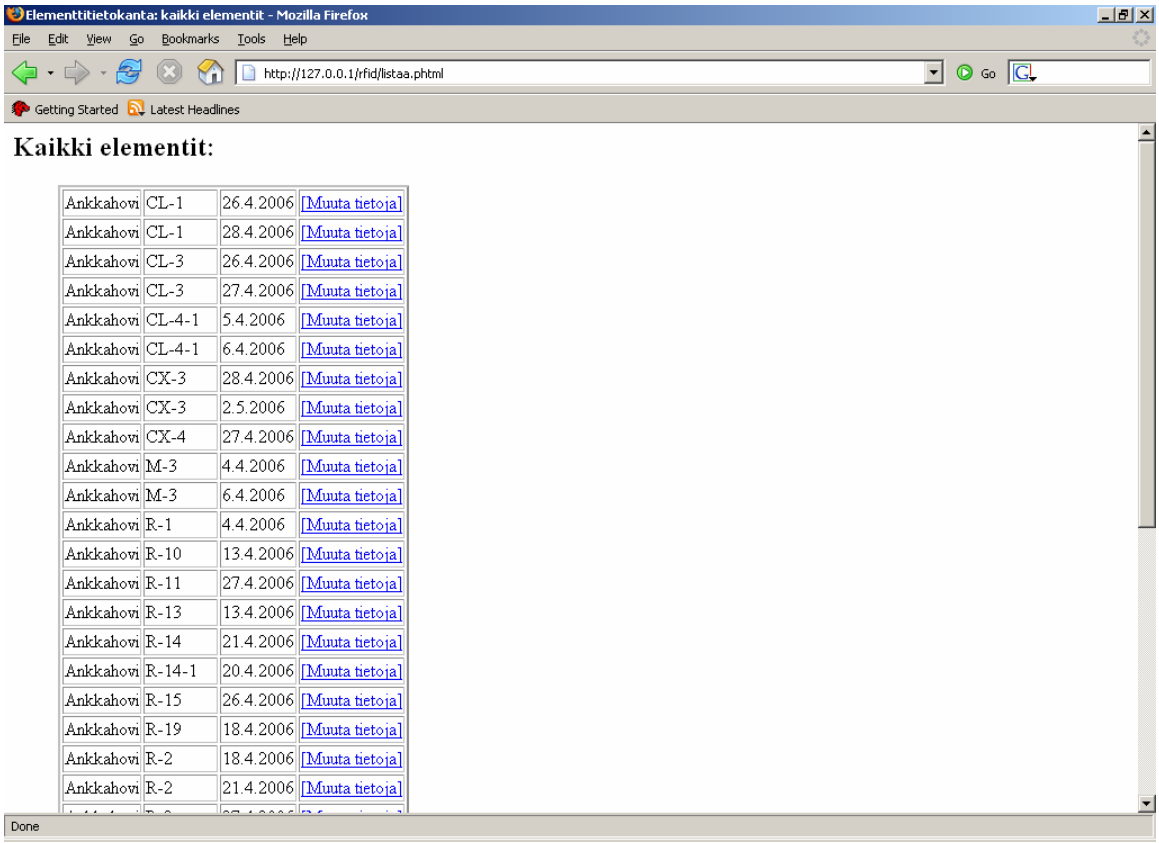
Tämän jälkeen oikean elementin tiedot ovat luettavissa selaimesta. Käyttäjä voi nyt lukea tarvitsemansa tiedot tai muokata elementien tietoja haluamallaan tavalla. Mikäli käyttäjä

muokkaa tietoja, täytyy uudet tiedot lähettää takaisin palvelimelle. Tällöin suoritetaan jälleen PHP–ohjelma, joka ottaa yhteyden tietokantaan ja tallentaa sinne uudet tiedot.

7.2.3 Käyttöliittymä

Yksittäisten elementtien tiedot tallennetaan siis tietokantaan. Tietojen lisäämiseksi, hakemiseksi ja muokkaamiseksi toteutettiin selainkäyttöinen käyttöliittymä. Näin ollen tietokone, jolla tietoja halutaan hakea, ei tarvitse tietojen käsittelyä varten erillistä ohjelmaa, vaan pelkkä www-selain riittää.

Käyttöliittymän toteuttamiseksi palvelinkoneella ajetaan tietojen tallentamiseen käytettävän tietokantapalvelimen lisäksi www-palvelinohjelmistoa. Perus www-palvelimen toiminnallisuuden lisäksi sivujen dynaamista luomista varten palvelinohjelmistolta vaaditaan kykyä ajaa PHP-ohjelmia. PHP:n avulla luodaan dynaamisesti www-sivuja jotka sisältävät tietokannasta haettuja elementtien tietoja. Käytännössä käyttöliittymä koostuu erilaisista lomakkeista, joilla tietoja voidaan hakea, selata, lisätä ja muokata. Kuvassa 25 nähdään esimerkki käyttöliittymästä. Tässä kuvassa nähdään listaus kaikista tietokantaan tallennetuista elementeistä. Käyttäjä voi valita listauksesta yhden elementin ja lukea tai muokata sen tietoja.



Kuva 25. Esimerkki käyttöliittymästä – kaikkien tallennettujen elementtien listaus

7.3 Siirrettävät tiedot

Projektin tavoitteena oli siirtää elementin tiedot rakennuspaikalle ja RFID-tekniikkaa hyödynnetään elementin tunnistamisessa. Tunnistamisen lisäksi se mahdollistaa tietojen siirron tunnisteen muistissa. Tunnisteen muisti ei kuitenkaan sovellu tietojen ainoaksi tallennuspaikaksi, sillä tällöin tietoja ei saada haltuun tunnistetta lukematta ja ne voidaan lukea ainoastaan elementin läheisyydessä. Elementin ollessa vaikkapa eri paikkakunnalla ovat tiedot saavuttamattomissa. Lisäksi riski tietojen häviämiseen on olemassa. Jos tunniste rikkoutuu jostakin syystä, tiedot katoavat. Tunnisteiden muistin määrä on myös rajoitettu ja näin ollen kaikkea mahdollista tietoa ei voida sinne kirjoittaa. Samoin rajoitettu muisti vaikeuttaa kirjoitettavan tiedon jäsentelyä. Rajoitetulla muistimäärällä on vaikeaa toteuttaa dynaamista järjestelmää, jossa siirrettävät tiedot voivat muuttua tapauksesta toiseen. Rajoitetulla muistimäärällä tiedot on tallennettava mahdollisimman pieneen tilaan mikä käytännössä se tarkoittaa tiukasti määriteltyä formaattia. Näin tunnisteeseen kirjoitettavien tietojen muutos tapauskohtaisesti ei ole mahdollista.

Tunnisteen muistin käyttö tiedon siirtoon on ongelmallista myös käyttöoikeuksien hallinnan kannalta. Miten voidaan varmistua siitä, että tietoja pääsevät lukemaan ja varsinkin kirjoittamaan ainoastaan sellaiset henkilöt, joilla on siihen oikeus. Käytetyt ISO15693–standardin mukaiset tunnisteet tarjoavat tietoturvan kannalta ainoana ominaisuutena kirjoitettujen tietojen lukitsemisen niin, että niitä ei lukitsemisen jälkeen voi enää kirjoittaa uudelleen. Tämä tarkoittaa samalla sitä, että kukaan ei voi kyseisiä tietoja muuttaa. Lukemista ei näillä tunnisteilla pysty rajoittamaan, vaan kaikki tunnisteeseen kirjoitetut tiedot ovat aina kaikkien sopivan lukulaitteen omistavien henkilöiden saatavilla. Saatavilla on myös tunnisteita joiden tiedot voidaan suojata avaimella, jota ilman niiden lukeminen ei onnistu. Tällöin ongelmana on, että kaikille henkilöille, jotka tunnisteita lukevat, on jaettava sama avain jolloin kaikilla heillä on myös samat oikeudet. Näin lukuoikeuksien jako tapahtuu kaikki tai ei mitään periaatteella eikä käyttäjiä voi jakaa oikeuksiensa puolesta erilaisiin ryhmiin.

Näistä syistä elementin tietojen pääasialliseksi tallennuspaikaksi valittiin tietokanta, josta ne voidaan hakea elementiin upotetun tunnisteen sarjanumeron perusteella. Näin voimme vapaammin valita tallennettavat tiedot ja jopa vaihdella niitä tapauksesta toiseen. Asiakasohjelma hakee kuitenkin vain tarvitsemansa tiedot. Samoin käyttäjäoikeuksien hallinta helpottuu kun voimme vaikkapa myöntää jokaiselle käyttäjälle oman käyttäjätunnuksen ja päättää siihen kuuluvat oikeudet.

Tässä projektissa elementistä talletettiin seuraavia tietoja. Ensinnäkin jokaisella elementillä on rakennustyömaakohtainen tunnistekoodi. Tämä koodi ei välttämättä ole yksilöllinen, vaan kaikki saman kohteen identtiset elementit varustetaan samalla koodilla. Koodin lisäksi talletettiin kohde, johon elementti on tarkoitettu, sen valupäivämäärä, ulkomitat sekä paino. Näistä tiedoista talletettiin testimielessä ulkomitat ja paino myös elementtiin upotetun tunnisteen muistiin.

7.4 Käytännön testit

Käytännön testeissä tunnisteita valettiin osaan yhden rakennuskohteen elementeistä. Kaikkiaan tunnisteita valettiin 29 ja niiden lukeminen testattiin valmiissa rakennuksessa. Elementtejä, joihin tunnisteita valettiin, oli kolmen tyyppisiä. Tavallisia *ulkoseinäelementtejä*, jotka koostuvat kahdesta betonikerroksesta (sisä- ja ulkopinta) sekä niiden välissä olevasta eristeestä. Toisena elementtityyppinä oli parvekkeiden välissä ja reunoilla käytettäviä *pielielementtejä*, joissa ei ole eristeitä, vaan ainoastaan betonia läpi elementin sekä kolmantena elementtityyppinä parvekkeen *lattiaelementti*.

Tunnisteet oli tarkoitus valaa vakiopaikkaan jokaisessa elementissä, jotta ne voitaisiin löytää valmiista elementeistä helposti ilman että niiden sijaintipaikkaa on merkitty elementin pintaan. Vakiopaikan määrittäminen ei ollut helppoa, sillä elementit ovat hyvinkin erilaisia ja tunnisteen tulisi olla helposti löydettävissä niistä kaikista. Tämän lisäksi tunnisteen tulisi olla luettavissa elementin ollessa niin tuotannossa, varastossa kuin asennettunakin. Tämä luo ongelmia sillä elementin asento on eri sen ollessa eri paikoissa. Esimerkiksi parvekkeen lattiaelementti varastoidaan pystyasennossa, mutta asennettuna paikalleen se on tietenkin vaaka-asennossa. Elementit varastoidaan niin sanottuun kampaan, jossa ne ovat pystyasennossa, toisesta päästä kiinni telineessä, ”kammassa” hyvin lähellä toisiaan. Jotta elementissä oleva tunniste on luettavissa, on sen sijaittava joko elementin päässä tai ainakin hyvin lähellä sitä, jotta tunniste voidaan lukea elementtien välistä.

Tunnisteen sijoituspaikka valittiin seuraavasti. Pääsääntöisesti tunniste sijaitsee varastoasennossa 120 cm korkeudella maasta ja 20 cm elementin vasemmasta reunasta. Sijoituspaikka on nyt sellainen, että tunnisteen lukemisen pitäisi onnistua tuotannon eri vaiheissa, oli elementti missä asennossa tahansa.

7.4.1 Ulkoseinät

Tunniste sijoitetaan *sisäseinän* puolelle, jotta lukeminen onnistuu valmiissa rakennuksessakin helposti. Sijoituspaikka on elementin *vasemmassa* reunassa *120 cm* korkeudella lattiapinnasta ja *20 cm* elementin reunasta.

7.4.2 Parvekelaatat

Tunniste sijoitetaan elementin *yläpintaan* niin että se on *varastointiasennossa* elementin *vasemmassa* reunassa *120 cm* korkeudella elementin alareunasta ja *20 cm* elementin reunasta.

Parvekkeiden pielissä käytettiin samoja sääntöjä tunnisteiden sijoittamiseen kuin ulkoseinissäkin. Pielissä ongelma on se, että niillä ei ole samalla lailla sisä- tai ulkopuolta kuten seinäelementeissä. Tästä syystä tunnisteen sijoituspaikka saattoi osua satunnaisesti parvekkeen sisä- tai ulkopuolelle. Parvekkeiden välisissä pielissä tämä ei ole ongelma, mutta talon ulommaisissa pielissä ongelmia saattaa esiintyä, mikäli tunniste on osunut elementin ulkosivuun.

Elementit valmistetaan elementtipedeillä vaaka-asennossa. Näin ollen tunnisteen sijoittamispinta voi olla valmistusvaiheessa joko sen ylä- tai alapinta. Tyypillisesti ulkoseinäelementtejä valmistettaessa seinän ulkopinta on alempana, eli sisäpinta johon tunniste asennetaan, jää yläpinnaksi. Parvekkeen lattiaelementeissä taas lopullinen yläpinta on valmistuksen aikana tyypillisesti elementtipetiä vasten sijaitseva alempi pinta. Tunniste on tarkoitus sijoittaa mahdollisimman pintaan. Mikäli sijoituspinta on valmistusvaiheessa ylempi pinta, on asennus helppoa. Tunniste vain upotetaan valun lopuksi oikeaan kohtaan hieman betonin pinnan alle. Mikäli sijoituspinta taas on valmistuksen aikana alempi pinta, on tunniste kiinnitettävä paikalleen ennen betonin valamista. Tällöin tunniste kiinnitettiin samanlaisiin muovisiin ”koroke-paloihin”, millaisten päälle raudoituskin rakennetaan. Tällöin tunniste sijoittuu noin 35 mm päähän elementin pinnasta. Tämä etäisyys ei vielä ole ongelma testeissä käytetylle lukulaitteelle.

Tunnisteiden sijoittaminen osoittautui ongelmalliseksi, sillä pelkän elementtipiirustuksen perusteella ei pysty päättelemään millaiseen paikkaan elementti sijoittuu valmiissa rakennuksessa ja jääkö tunniste todellisuudessa sellaiseen paikkaan, että sen voi jälkikäteen lukea. Esimerkiksi parvekkeiden täysin identtisiä parvekkeiden pieliä valmistuu rakennukseen useita ja yksittäisen elementin lopullista sijoituspaikkaa ei tiedetä etukäteen. Näin ollen ei välttämättä tiedetä kumpi puoli pielestä jää parvekkeen sisä- ja kumpi ulkopuolelle. Toisaalta elementin eteen saattaa tulla valmiissa rakennuksissa muita rakenteita, jotka estävät tunnisteen lukemisen. Tällaisista tilanteista pitäisi olla tieto tunnisteen sijoituspaikkaa valitessa.

Tunnisteen paikka on siis tiedossa, mutta sitä ei ole merkitty millään tavalla, eli tunnisteen täsmällistä sijoituspaikkaa ei pysty elementistä näkemään. Tästä huolimatta tunnisteiden löytäminen onnistuu nopeasti ilman sijoituspaikan mittaustakin. Lukulaitteen ei tarvitse olla täsmällisesti tunnisteen päällä löytääkseen sen, ja etsiminen on helppoa, kun lukulaite ilmoittaa tunnisteen löytymisestä äänimerkillä.

7.5 Testikohde

Kohde johon testitapauksena käytetyt elementit valmistettiin, oli As Oy Ankkahovi Vantaan Korsossa. Kohde koostuu kolmesta viisikerroksisesta kerrostalosta joissa asuntoja on yhteensä 59 alkaen 32,5 neliön yksiöistä 94,5 neliön perheasuntoihin.

Kuva 26. Testikohde

Testitapauksena käytettiin ensimmäisenä valmistuvaa A-taloa, jonka elementteihin upotettiin RFID-tunnisteita. Käytännön syistä kaikkiin elementteihin ei upotettu tunnisteita, vaan ainoastaan osa otettiin mukaan testiin. Rakennuspaikalla elementit tunnistettiin tunnuskoodin perusteella. Samalla työmaalla saatetaan käyttää identtisiä elementtejä useassa eri paikassa, siis eri kerroksissa ja jopa eri rakennuksissa. Näillä kaikilla identtisillä elementeillä on sama tunnus. Koska tunnus on sama, ei etukäteen voida tietää varmasti, mihin kyseinen elementti tulee valmiissa rakennuksessa sijoittumaan ja näin ollen vaikka jokin elementti on elementtitehtaalla valmistettaessa suunniteltu asennettavaksi tiettyyn paikkaan, voidaan se käytännössä asentaa muuallekin.

Elementtitehtaalla elementteihin upotettiin kaiken kaikkiaan 29 tunnistetta. Näistä yhdeksän upotettiin parvekelaattoihin, kaksi parvekkeen pieliin ja 18 seinäelementteihin. Tunnisteiden lukemista testattiin myöhemmin rakennuspaikalla kun elementit oli jo asennettu paikalleen. Kaiken kaikkiaan tunnisteista löydettiin vain 17. Mutta lukua pudottaa se, ettei kaikkia tunnisteita päästy lukemaan joko siitä syystä, että tunnisteen edessä oli muita rakenteita tai siksi, että mittauspäivänä elementit olivat rakennustarvikkeiden alla. Kun nämä tunnisteet,

joita ei päästy mittaamaan otetaan luvuista pois, jäi tunnisteita löytämättä ainoastaan kaksi. Näille voi selitys löytyä siitä, että täysin identtisiä elementtejä käytetään saman työmaan eri rakennuksissa ja tunnisteita mitattiin ainoastaan ensimmäiseksi valmistuneesta A-talosta. Näin ollen tunnisteella varustetut löytymättä jääneet elementit ovat luultavasti jossakin muualla samalla työmaalla. Yhtään varmaa epäonnistunutta tunnisteen lukemista ei siis tapahtunut. Yhteenveto lukutestien tuloksista on nähtävissä taulukossa 8.

Taulukko 8. Yhteenveto lukutesteistä rakennuspaikalla

	Asennettu	Ei mitattu	Löydetty	Ei löydetty
Parveke	9	7	1	1
Pieli	2		1	1
Ulkoseinä	18	3	15	
Yhteensä	29	10	17	2

Kaikkein suurimmat ongelmat lukemisessa olivat parvekkeen lattiaelementtien kanssa. Ongelmana oli tunnisteiden sijoituspaikan epäonnistunut valinta. Kaiken kaikkiaan viidessä elementissä tunniste asetettiin paikkaan, jonka päälle valmiissa rakennuksessa sijoittuu ylempää parveketta tukeva tolppa. Näistäkin elementeistä kahden elementin tunnisteen lukeminen testattiin jo elementtitehtaalla heti valmistuksen jälkeen onnistuneesti. Tämän lisäksi kahta muuta tunnistetta ei päästy lukemaan, sillä kyseiset parvekkeet olivat täynnä rakennustarvikkeita lukutestien suorituspäivänä. Lopulta tunniste löydettiin ainoastaan yhdestä elementistä ja löytämättä jäi yksi. Syy löytämättä jäämiseen on oletettavasti se, että kyseinen elementti on asennettu johonkin toiseen taloon ja siksi sitä ei löydetty.

Parvekkeen pielielementteihin tunnisteita upotettiin ainoastaan kaksi. Näistä elementeistä toinen löydettiin ja toista ei. Tässäkin tapauksessa samanlaisia elementtejä käytetään useammassa rakennuksessa, ja on hyvin mahdollista, että löytämättä jäänyt tunniste on asennettu eri rakennukseen.

Parhaiten tunnisteiden lukeminen onnistui ulkoseinäelementeistä. Niihin upotettiin tunnisteita yhteensä 18 kappaletta joita löydettiin 15. Kolme tunnistetta joita ei löydetty, oli asennettu huonoon paikkaan, sillä valmiissa rakennuksessa niiden eteen osui kuilu putkia varten. Yhtään tunnistetta, jonka lukemista päästiin testaamaan, ei siis jäänyt löytymättä.

Kaiken kaikkiaan tunnisteita jäi löytymättä siksi, että ne olivat esteiden takana kymmenen kappaletta. Tunnisteiden sijoituspaikka on siis valittava huomattavasti huolellisemmin, mikäli ne otetaan tuotantokäyttöön. Löytämättä jäi ainoastaan kaksi elementtiä, mutta ne on mahdollisesti asennettu toisiin rakennuksiin, sillä niissäkin on käytössä täysin identtisiä elementtejä. Voidaan sanoa, että tunnisteiden lukeminen onnistuu kyllä periaatteessa, mutta käytännössä sijoituspaikan valinta on kriittinen, mikäli tunniste halutaan lukea vielä valmiissa rakennuksessa.

8. YHTEENVETO JA JOHTOPÄÄTÖKSET

Tässä työssä tutkittiin, onko betonielementtien tunnistaminen mahdollista käyttäen RFID-tekniikkaa. Ensimmäisessä vaiheessa kartoitettiin markkinat, jotta selvisi, minkälaisia tunnisteita ja lukulaitteita on tarjolla ja mitkä niiden ominaisuudet ovat. Tässä vaiheessa järjestettiin esitestit. Esitestien perusteella valittiin jatkotutkimuksiin ISO 15693-standardin mukaisia tunnisteita sekä niiden kanssa yhteensopiva lukulaite. Näitä tunnisteita testattiin ensin laboratorio-olosuhteissa, jotta betonin ja muiden väliaineiden vaikutukset lukutapahtumaan selviävät ja lopulta näitä tunnisteita upotettiin tuotannossa oleviin betonielementteihin. Betoniin upottamisen jälkeen tunnisteiden tietojen lukemista testattiin ensin tehtaalla ja lopulta rakennuksen pystytyksen valmistuttua rakennuspaikalla.

Laboratoriossa tunnisteiden lukemista testattiin eri väliaineiden läpi ja suurin mahdollinen lukuetäisyys mitattiin. Tunnisteiden lukeminen onnistui niin betonin, veden kuin jäänkin läpi. Lukuetäisyydet tippuivat näiden aineiden vaikutuksesta jonkin verran, mutta tunnisteen lukeminen onnistui siitä huolimatta. Ainoa testattu aine, joka estää lukemisen kokonaan on teräs. Tunnisteen lukeminen ei onnistunut ollenkaan, mikäli tunniste on teräksen takana, tai kokonaisuudessaan kosketuksissa teräkseen. Myös tunnisteen läheisyydessä sijaitseva teräs laskee lukuetäisyyksiä, mutta ei estä tietojen lukemista kokonaisuudessaan.

Lopulta RFID tekniikan käyttöä testattiin todellisessa rakennusprojektissa. Osaan erään rakennustyömaan betonielementeistä upotettiin RFID tunnisteita. Tunnisteisiin kirjoitettiin kyseisten elementtien mittatiedot. Tämän lisäksi elementin tiedot kirjoitettiin tietokantaan, johon kirjoitettiin lisäksi kyseiseen elementtiin upotetun tunnisteen sarjanumero. Näin elementin tiedot voitiin hakea näkyville lukemalla sen sisältämän tunnisteen sarjanumero. Käytännön testeissä tunnisteiden tietojen lukemista testattiin rakennuksen pystyttämisen jälkeen. Testit onnistuivat hyvin, tosin osa tunnisteista jäi löytymättä epäonnistunen tunnisteen sijoituspaikan takia, sillä tunnisteet sijaitsivat valmiissa rakennuksessa paikassa, josta niitä ei päästy lukemaan. Kuitenkaan kaikki tunnisteet, joiden lukemista päästiin yrittämään, onnistuttiin lukemaan ja näin ollen testit onnistuivat hyvin.

Testien lopputuloksena voidaan todeta, että RFID-tunnisteet soveltuvat teknisesti betonielementtien tunnistamiseen Käytännön soveltamisen kanssa on tosin vielä ongelmia, jotka täytyy ratkaista ennen kuin tekniikka voidaan ottaa tuotantokäyttöön elementtiteollisuudessa.

LÄHTEET

[1] Finkenzeller, Klaus. *RFID handbook : fundamentals and applications in contactless smart cards and identification*. Chichester : Wiley, 2003

[2] Flores, J.L.M., Srikant, S.S., Sareen, B., Vagga, A. *Performance of rfid tags in near and far field*. IEEE International Conference on Personal Wireless Communications, 23-25 Jan. 2005 Sivut 353 – 357

[3] Want, Roy. *The Magic of RFID*. Queue Volume 2, Issue 7 (October 2004).Sivut: 40 – 48. ISSN:1542-7730

[4] Jae-Ryong Cha, Jae-Hyun Kim. *Novel Anti-collision Algorithms for Fast Object Identification in RFID System*; Proceedings of 11th International Conference on Parallel and Distributed Systems, 20-22 July 2005. Volume 2. Sivut 63 – 67

[5] Hardgrave, Bill C, Waller, Matthew, Miller, Robert. *Does RFID Reduce Out of Stocks? A Preliminary Analysis*. 2005. Information Technology Research Institute, Sam M. Walton College of Business, University of Arkansas. ITRI-WP058-1105

[6] Koroneos, George. *Securing the Supply Chain with RFID*. Pharmaceutical Technology, September 2005. Sivut 48-55.

[7] Kontnik, Lewis T; Dahod, Shabbir: *Safe and Secure*. Pharmaceutical Executive; September 2004. Sivut 58-66

[8] Rieback, M.R., Crispo, B., Tanenbaum, A.S. *Is Your Cat Infected with a Computer Virus?* Pervasive Computing and Communications, PerCom 2006. Fourth Annual IEEE International Conference on 13-17 March 2006. Sivut 169 - 179

[9] Garfinkel, Simson; Rosenberg, Beth: *RFID – Applications, security and privacy*. Addison Wesley. 2005. ISBN 0-321-29096-8.

[10] Juels, Ari, Rivest, Ronald L., Szydlo, Michael. *The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*. Proceedings of the 10th ACM conference on Computer and communications security

[11] O'Halloran, M., Glavin, M. *RFID Patient Tagging and Database System*. International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006. International Conference on 23-29 April 2006 Sivu162 DOI 10.1109/ICNICONSMCL.2006.187

[12] Rantala, Ari: *PHP*. Docendo Finland Oy, Porvoo, 2002. ISBN: 951-846-147-3

[13] Heinisuo, Rami: P*HP ja MySQL – Tietokantapohjaiset verkkopalvelut*. Talentum, Jyväskylä 2004. ISBN: 952-14-0847-2

[14] Ruff, T.M., Hession-Kunz, D., *Application of radio-frequency identification systems to collision avoidance in metal/nonmetal mines*. Industry Applications, IEEE Transactions on Volume 37, Issue 1, Jan.-Feb. 2001 Sivut 112 – 116 DOI 10.1109/28.903133

[15] Aulds, Charles. *Linux Apache Web Server Administration*. SYBEX. 2000.

[16] Netcraft homepage: http://news.netcraft.com/

[17] Annalee Newitz. *The RFID Hacking Underground*. Wired. May 2006. Sivut 166-171

[18] Jonathan Westhues. *Demo: Cloning a Verichip*. Verkossa: http://cq.cx/verichip.pl

[19] EPCglobal Inc.Homepage. http://www.epcglobalinc.org/

[20] Lahiri, Sandip: *RFID Sourcebook*. IBM Press 2005. ISBN 0-13-185137-3

[21] Glover, Bill & Bhatt, Himanshu: RFID Essentials. O'Reilly 2006. ISBN 0-596-00944-5

[22] Mifare homepage. verkossa: http://mifare.net/

[23] Kfir, Z. Wool, A. *Picking Virtual Pockets using Relay Attacks on Contactless Smartcard*. Security and Privacy for Emerging Areas in Communications Networks, SecureComm 2005. First International Conference on 05-09 Sept. 2005 Page(s):47 – 58 DOI 10.1109/SECURECOMM.2005.32

[24] Hancke, G.P., Ruff, T.M., Hession-Kunz, D. *Practical Attacks on Proximity Identification Systems (Short Paper)*.;Security and Privacy, 2006 IEEE Symposium on 21-24 May 2006 Page(s):328 – 33 Digital Object Identifier 10.1109/SP.2006.30

[25] Poliisin passia käsittelevät kotisivut. verkossa:www.poliisi.fi/passi

[26] Sisäasiainministeriön kotisivut. verkossa www.intermin.fi