Thesis
On
Security Issues in RFID

By

Ankur

KTH
VETENSKAP
OCH KONST

ROYAL INSTITUTE
OF TECHNOLOGY

A thesis submitted in partial fulfillment of the requirements for the degree of
M.Sc in Information Technology Specialization in ICT Entrepreneurship

Approved by: Dr. Terrence Brown

Table of Contents

Acknowledgement

This thesis represents my process of becoming. It is appropriate for me to thank those who have been part of my journey.

First and foremost I would like to give special thanks to the examiner and supervisor Dr. Terrence Brown for his help and guidance during the project work. His phrases have always bought elegance to my fractured thoughts.

I am also thankful to my family without whom I would have been lost and whose love and unwanted support brought me comfort and warmth.

I would also like to thanks to all my friends and by association friendships, whose faith in me pushed away self-doubt and made me smile.
I would also like to extend my thanks to the School, for providing me the opportunity to make this thesis.

Last but not the least I would like to thank to all the interviewees, without whose help this would have not been completed.

Abstract:

Radio frequency identification (RFID) is a technology with a great potential in many industries and a wide spectrum of possible uses. Industries main aim is to make it possible to trace an individual product through the whole process, so it is possible to see where the product has been at a specific time.

The purpose of this report is to give an overview of the RFID technology and how it is working. This report will give some suggestions on which type of RFID system that is suitable. Unfortunately RFID also brings with it some of its faults which can result in security threats. This paper is a result of a research conducted on the subject of security problems in RFID enabled in industry. It firstly explains in detail the paths and methods this research used and elaborates more in depth about the research problem during which the research question and its scope are defined. In this part 'What can companies do to avoid or combat security problems of RFID in their processes?' is selected as a main research question?'

Following parts give introduction to the technology, its application and other issues addressed in the research to ensure better understanding of the subject. Current research and available literature are used do define problems with security in RFID which is then joined with some practical experiences and experts opinions to create final findings, conclusions and recommendation. Conclusions and recommendations are created in a helpful way to provide clear and useful overview of the potential problems that RFID enabled organizations might face and it also gives some idea (not all possible solutions are addressed) on how to avoid or combat these problems .

What this research concentrates on is issues related to potential security problems that this technology inevitably brings in its current stage of development.

Due to the wide applicability and many different aspects of this technology it is not possible to address everything related to security, souse of this technology in corporate world like for e.g. Logistics, track and tracing of products were chosen as narrower perspective and as probably most vulnerable part of RFID implementation spectrum. Focusing on influence of RFID implementation in corporate security is much more realistic and achievable considering limitation factors of writing a master's thesis. The aim of the research is also to provide recommendation for the organizations to give them a clear picture of the RFID system and possible security threats and their solutions.

1 INTRODUCTION

In this chapter we will explain the background for this thesis. This will give a clear picture of the main purpose of the thesis.

1.1 Background

The Radio Frequency Identification (RFID) technology was established in the late 70’s but it is in recent time that companies have begun to understand its many benefits both for production and distribution. One of the leading organizations who have started to look into the RFID technique is the American Department of Defense. Other large companies that are doing or have done pilot projects with the RFID technique are; Wal-Mart (USA), Metro (Germany), Marks and Spencer (UK) and Benetton (Italy). Ford , Air France ,DHL .

An increased number of organizations understand that this technology is going to be an evolution in the same way that the barcodes where when they were presented. But one has to remember that the RFID-technology is in its childhood and it is not fully developed to fit all different markets yet. There are still a lot of questions to be answered; the technology has to be tested in smaller scales, a global frequency standard has to be set and the technique has to become less expensive before it gets its breakthrough. However we think that there will be a breakthrough and the question is do the companies dare to wait…?

This information could be used to see what benefits it can give to the organizations *and possible security threats related to organization policies and their solutions.*

1.2 Purpose

The purpose of this thesis is to *investigate the RFID systems and possible security threats related to organization policies and their solutions.*

2 Method

To gather information about RFID we used literature about the technology and the use of the technology in current applications. We also used the Internet as a source of information and to find RFID manufacturers. We contacted many of these manufacturers and some of them we held interviews and had email correspondence with.

3 Introduction to RFID Technology

Acronym for Radio Frequency Identification
. Enables automatic identification (unique) of physical objects through radio interface

3.1 RFID Systems

Three main components:

1 Tags, or transponders, carry identifying data.
2 Readers, or transceivers, read or write tag data.
3 Back-end databases associate records with tag data collected by readers.

Every object to be identified in an RFID system is physically labeled with a tag.

- . Tags consist of a microchip attached to an antenna.
- Readers query tags via radio signals and the tags respond with identifying information.

4.1 RFID history

In the 1930.s, the Army and the Navy in USA were interested to find new ways to identify targets on the ground, at sea and in the air. During World War II, the allied wanted to distinguish its own aircraft from the enemy aircraft. At that time they developed the Identification Friend-or-Foe (IFF) system.
The IFF system was developed so that a transponder was attached to an allied aero plane. This transponder received a signal and sent an adequate signal back. This technology is the basis for the world's air traffic control systems today.
Because of the high cost and large size of components, the early use of radio identification through the 1950.s was generally limited to the military and research labs. When more compact and cost-effective technologies, for example IC and the microprocessor, arrived, RFID as it is known today were developed.
In the late 1960.s and 1970.s companies introduced new uses for RFID for less complex and more widely used applications. The most known of these applications is the Electronic Article Surveillance (EAS) equipment to protect inventory items such as clothing in department stores. These systems used a 1-bit transponder, affixed to articles, which were designed to start an alarm when they came near a reader.
Another use of RFID that started at this time was to implement a transponder into the back of a cow. This was done to make it possible to track the cow's ID and its temperature for a better control of, for example, the cow's health.

The railroads in USA were involved after a bad attempt to use bar code technology to track rolling stock. They then turned to RFID for a possible solution to many problems caused by the unique environment of their industry. The use of Radio Frequency (RF) has many benefits over bar code, for example longer read distance and the ability to read in direct sunlight. That is a problem with visual light or infrared-based systems like bar codes.

Some other applications were spun off from this original application including fleet vehicles, automatic toll collection on highways, access control to secured or monitored areas, and even the Remote Keyless Entry (RKE) systems now very common for automobile access. (www.members.surfbest.net)

The 1980.s became the decade for total implementation of RFID, because it was spread over the world. In USA, the greatest interest was in transportation, personnel access and for animals. Short-distance systems for industrial and business applications caught the greatest interest in Europe, though toll roads in some countries were equipped with RFID. Around the middle of this decade, the greatest efforts in RFID were changed from new applications to performance improvements, cost reductions and size decreasing. In 1991, Texas Instruments developed the modern RFID system. This system has become a vibrant platform for developing and implementing dozens of new classes of RFID applications. (www.aimglobal.org)

4.2 RFID today

Here we will discuss some of the RFID systems that are in use today.

4.2 Volvo

4.2.1 Volvo Construction Equipment AB, Cab Division

RFID already exists inside the VCE, Cab Div factory in Halls berg. It is a small RFID system with only one reader and one antenna. The RFID system is located in the automated system for welding cabs. The information on the tag consists of a serial number to let the system keep track of the fixtures in an automated storage. The robot welding system software now keeps track of the different fixtures, until one of them leaves the system robot.

The RFID system is a 13, 56 MHz system from EMS. The reader is a HMS 820 and the tags are HMS 150 and are of RW type with a range of 5 centimeters. When the tag on the fixture is read, the antenna is placed so the distance between antenna and tag is approximately 2 centimeters. The information is sent from the reader to a PC with a RS232 connection.

4.2.2 Volvo Trucks in Umeå

Volvo Trucks in Umeå makes cabs for trucks. They needed a system to track cabs in the factory. The system they had until they got the RFID system was a barcode system which only allowed them to see how many cabs there were in the factory at a specific time, not where they were. Volvo Trucks got two RFID systems, one in the paint shop and the other one in the trim shop, which they implemented in 2003, paint shop, and in the autumn 2004, trim shop. Both systems are closed systems, which means that the transponders never leave the factory and are reused. In the paint shop, the tag is placed on a skid that carries the cab during the process. The information on the tags are used by paint robots, so they know what type of cab it is and which paint program and which color the robot will choose. At the last stage of the paint shop, just before the cab is removed from the paint shop skid, the ID-number of the tag is printed out on a temporary barcode and placed on the cab. The system used in the paint shop, is a 13, 56 MHz system with RW tags. The readers are LRP 820 from EMS with a maximum reading range of 45 centimeters. The paint shop system includes 11 readers at the total price of 50 000 SEK. The tags are LRP 525 HTS from EMS that are a passive RW tags with 112 bytes of memory that can withstand high temperatures and the chemical substances used in the process. Volvo Trucks bought 700 tags at the price of 650 SEK a piece.

In the trim shop, the RFID system is used to keep track of the cabs in the trim line and which components that are to be placed on a particular cab. When the skid, with the cab on it, enters the first stage of the trim line, the barcode on the cab is scanned manually and the barcode information is linked to the tag on the skid in the database. The tag is then read 16 times during the trim line, before the tag is removed from the skid and taken back to the beginning of the process, ready to be used on another skid.

The system in the trim line is a LF system, 125 kHz, from Siemens that is called Moby F. The system uses two kinds of readers, Moby F SLA-81 with a reading range of 14 centimeters and Moby F SLA-82 with a reading range of 20 centimeters. The tag used is MDS F 125, which is a passive RO tag with a memory of 5 byte. These tags were bought at the price of 71 SEK apiece.

4.3 Volkswagen

At Volkswagen there is an RFID system that makes it possible to quickly locate a car in the holding lot. The system is also used for tracking the car through pre-delivery activities. To make this possible, Intelligent Long Range (ILR)-enabled wireless technology is used.

ILR RFID technology is based on long-range active tags.

The ILR technology optimizes the workflow for the delivery of manufactured cars to the customer. In an electronic routing slip, which is temporarily attached to the car, are all tasks involved in the delivery process stored. Each time a car is moved through an ILR-enabled process station, its location and current status can automatically be immediately known by the worker. (www.identecsolutions.com

The system works like this:

A tag is placed on the rear-view mirror when the car leaves the production area. To the tag, an electronic routing slip is written. This slip includes the vehicle ID and pre-delivery tasks. When the car has been tagged, it is moved to a holding parking lot. In this parking lot, an ILR-enabled van with a laptop drives around. The tag inside the car begins to blink and the laptop emits a beep when a desired car is approached by the van. Then the car is brought to a cleaning station, where it is automatically detected entering and leaving this area and the status of the tag is automatically updated. This detection and updating procedure is also applied when the car is brought to a storage facility. When the car is ready for delivery, the dimension of the car's wheelbase is read from the tag when it is passing through an ILR-enabled gate. This tag information is then used to automatically adjust the tracks on the transporting platform and to open the gate. Then the ILR-enabled platform will be activated and takes the car to the car towers. When the car is delivered to a customer, the tag is removed and re-used. (www.identecsolutions.com)

4.4 Saab

With the use of RFID system, every car manufactured by Saab is given its own unique identity from the beginning. The identity is provided in form of a data tag, which follows the car through the whole production plant. This system is to guarantee that the customer receives the right car. In the body shop, the data tags communicate with the individual reading stations at long distance, via microwaves. When the cars arrive to the paint shop, the tags will be exchanged with punched barcode plates. To identify these barcode plates, barcode readers are used in the paint shop. In the final assembly area, each car is transported on a carrier with a data tag mounted underneath. Antennas mounted on the floor in the middle of the line, identify the tag.
(www.baumer.se)

4.5 Wal-Mart

Wal-Mart, the world's largest retailer, decided that their 100 biggest suppliers should tag their products at January 2005. At January 2006, 300 of their biggest suppliers had tagged their products that they were delivering to 500 different Wal-Mart stores through five distribution centers. At January 2007 Wal-Mart expects that 600 suppliers will deliver their RFID tagged products to 1000 Wal-Mart stores. The system that Wal-Mart uses is in the UHF frequency. They have been using EPC Class 1. Generation 1 tags, but began the change to the Generation 2 tags in January 2006, The Generation 1 tags should be gone by June 30, 2006. In 2005, the University of Arkansas was doing a 29-week study, at Wal-Mart, on the out-of-stock merchandise in 12 pilot stores with RFID technology and 12 control stores without RFID. The study showed that the RFID equipped stores were 63% faster to replenish the out-of-stock items than the control stores. (www.idtechex.com)

5 RFID Technology

5.1 Introduction to RFID

Radio Frequency Identification (RFID) is a way for automatically identification of objects with radio waves, like a barcode that uses radio waves instead of light. A RFID system has a few major components, a reader with an antenna, a tag and a database, often a Personal Computer (PC) with connection to a larger network.

The tag is placed on the object that is to be identified. The tag contains the suitable information of the object. The reader has a number of different responsibilities like powering the tag, identify the tag, read and sometimes write data to the tag. The reader also communicates with the database in which the information from the tags will be processed.
When the object that is tagged comes in a reader's interrogation zone (reading zone), where the tags are being read, and the reader sends out a radio wave to the tag. The tag powers up and sends back its information to the reader, in some cases new information is sent from the reader to the tag. The reader sends the information to a database that processes the data from the tag in a suitable way. Because RFID is using radio waves it is not necessary to have a line of sight between the reader's antenna and the tag.

The distance between the transponder and reader depends on which coupling and frequency that are used. It is possible to achieve distances from a few centimeters up to hundreds of meters. The speed which the data can be transferred between tag and reader is also depending on which frequency that is used; lower frequencies can not transfer data as fast as the higher frequencies, due to the higher clock frequency allowed in the higher frequencies. This means that if it is necessary to read many tags at the same time a higher frequency is preferred. (www.morerfid.com)

5.2 Tags

The tag also known as the transponder, from the term's **trans**mitter and res**ponder**, holds the data that is transmitted between the tag and the reader. A tag consists of an Integrated Circuit (IC) with memory and an antenna. A tag can perform some basic tasks like read or write data to its memory. When a tag is in a reader's interrogation zone the data from its memory is retrieved and transmitted to the reader.

5.2.1 Tag formats

Tags come in many shapes and sizes. The reading range of the different tags are depending on which frequency that are used and the power level that are transmitted from the reader. The tags also differ in memory capacity and

temperature survivability. Almost all tags are encapsulated for durability against shock, moist, dirt and chemicals, but there are also cheaper tags without encapsulation. (www.ems-rfid.com)
The size of a tag depends primarily on two things, whether the tag have a battery or not and the size and shape of the antenna. The size and shape of the antenna depends on which frequency that is used. (www.rfidjournal.com)

5.2.1.1 1-bit transponder

The simplest of all tags is the 1-bit transponder. The 1-bit transponder is used in Electronic Surveillance System (EAS). The 1-bit tag can only represent two states 1 and 0, which means that the system only has two states as well, tag in readers interrogation zone or no tag in readers interrogation zone, there are no identification done. Despite of the 1-bit transponder limitations they are very widespread and its main application is anti-theft systems in shops.

5.2.1.2 Glass housing

A glass tag is encapsulated in glass. The glass tag is mostly used for animal identification. The tag gets inserted under the skin of the animal and can later be read, or written, from the outside. These tags use the lower frequencies so the electromagnetic wave can penetrate the animal's tissue.

5.2.1.3 Disks and coins

A very common construction is the so-called disk (coin), a tag in round injection molded housing with a diameter ranging from a few millimeters to several centimeters.

5.2.1.4 Labels

On a label the antenna is printed, etched or punched on a thin paper/polyester substrate with a chip. They are very flexible and can easily be attached to any products. They are less resistant to environmental conditions than the encapsulated tag but much cheaper. The labels provide low-cost benefits in open systems. When a label is involved in an open system it is attached to the product somewhere in the supply chain but never removed, so when it reaches the consumer it will never be reused. The labels can also be printed with all existing formats and layouts of text, barcodes and graphics. These printers also write information to the tags. (www.zebra.com)

5.2.1.5 Smart cards

Smart card, or contact less smart card, often looks like a normal credit card. There are three types of smart cards close-coupling smart card, proximity-coupling smart card and vicinity RFID technology Investigation of the RFID technology coupling smart card. The close-coupling smart cards have extremely short reading range and are often used for payment in public transportation like buses, planes subways. Proximity coupling smart cards have a reading range of a few centimeters, they are often used for large public gatherings that requires access control like sport events or concerts. Vicinity-coupling smart cards are designed to have a reading range up to a half meter or so, they are used as controlled access cards in office buildings.

5.2.2 Special purpose tags

5.2.2.1 Sensor tags

A sensor tag is not only designed to read or write from its memory, it can also perform simple tasks like measure air pressure, temperature or the presence of bacterial agents. A sensing device is packed together with the tag to record whatever it was designed to monitor. The challenge is when you would like a passive sensor tag. This means that the sensor only has power when the tag is in a reader's interrogation zone. That means that the sensor only can record the conditions for a very brief period of time and with a very limited power. Sensor tags are mostly active.

5.2.2.2 Chip less tags

A chip less tag is, as it sounds, a tag without a chip. They are therefore passive and most of the technologies involve the idea of encoding unique patterns on the surface of the tag that reflects the radio waves.

5.2.2.3 Encrypted tags

The encrypted tag is used whenever you are looking for a secure system like payment systems, ticketing or when you store company sensitive data on the tags like process flow.

5.2.3 Tag types

There are three types of tags passive, active and semi-active.

5.2.3.1 Passive

A passive tag does not have a battery; they use the energy that the electromagnetic wave from the reader induces in the antenna to power up the chip and to transmit the data back to the reader. Passive tags reflect energy from the reader or receive and temporarily store the energy in order to generate the tag response to the reader.

5.2.3.2 Active

An active tag has its own power source, typically a battery, to run the chip and to transmit the data to the reader. An active tag allows very low-level signals to be received and can still generate high-level signal to be transmitted back to the reader.

The active tag lies in sleep-mode until it gets a wake-up signal from the reader. As soon as the tag gets the wake-up signal the data carrier gets into operating mode. After the completion of the data transaction the tag gets into sleep-mode again. Because the active tag has a battery onboard they can transmit data without requiring a reader to power them. They have therefore much longer reading range then a passive tag. On the other hand because they have a battery they have finite lifetime.

5.2.3.3 Semi-active:

A semi-active, or semi-passive depending on the manufacture, also has an onboard battery. The battery in this case is only used to operate the chip. Like the passive tag it uses the energy in the electromagnetic field to wake up the chip and to transmit the data to the reader. These tags are sometimes called Battery Assisted Passive (BAP).

5.2.4 Tag memory

Transponders with memory functions range from simple RO tags to tags with intelligent crypto logical functions. There are tags available with memory ranges between a few bytes up to around 4MB of memory. It depends on what type of tag, passive or active, you chose to use and what standard you will follow. More and more companies are following the Electronic Product Code (EPC) standard that allows 96 bits of memory.

5.2.4.1 RO

A Read Only (RO) tag has a pre-programmed serial number written on its memory. The serial number is incorporated during chip manufacturing. The user can not alter this serial number or write new data to the tag. When the tag enters a reader's interrogation zone it will instantly start to send out its unique identification number and it will do so continuously until it is out of the reading zone. The data communication is unidirectional; data transmission from the reader to the tag is not possible. When using RO tags you need to connect the serial number of the tag with which product it involves with appropriate software.

5.2.4.2 RW

With a Read Write (RW) tag you can write new information to the tag or write over existing information. It is only possible to write information to the tag when it is in a reader's interrogation zone. You can of course also read information from the tag. RW tags usually have a pre-programmed serial number that can not be written over. But unlike the RO tags an RW tag also have a memory space where the user can put his own information. An RW tag has limited write cycles depending on which type of memory it is using.

5.2.4.3 WORM

A Write Once Read Many (WORM) is a tag which is something between an RO and an RW. You can, which the name indicates, write to the tag one time and read it as many as you like. When you have written to the tag the data on the tag becomes locked and you can only read from it.

5.2.5 Memory types

The chip size of the data carrier is primarily determined by its memory capacity. If you have an RO tag you only have a serial number written on its memory. This serial number is defined at the manufacturing stage by the chip mask or permanently burnt into the memory by a laser. Further data about the product in a RO system is kept in the software of the controlling computer. If the intentions are to write data to the tag, a tag with Electrical Erasable Programmable Read Only Memory (EEPROM), Random Access Memory (RAM) or Ferro electrical Random Access Memory (FRAM) is required. The most common type of memory in RFID system is EEPROM.

5.3 Readers

An RFID reader, also called interrogator, has the corresponding task as a barcode reader and that is to read data from an information carrier. The biggest different between these are that the barcode reader only can read one barcode at the time and visual connection is required. An RFID reader can normally read multiple tags in the read range at the same time, depending on which frequency range that is used.

In a simple way you can say that the reader is a radio frequency transmitter and receiver, controlled by a microprocessor or a digital signal processor. An antenna is attached to the reader and is used to capture data from tags. The data is then sent further to a computer for processing. Readers come, like tags, in a large number of different sizes and features. Readers can be affixed in a stationary position, for example beside a conveyer in a factory, portable, integrated in a mobile computer, and even embedded in electronic equipment. More about the different types will be discussed later in this report.

5.3.1 Reader types

A reader can be designed in several different ways, depending on the application.

5.3.1.1 Reader with internal or external antenna

Readers with internal antenna are often simpler and are used in applications where for example single tags are read. To a reader with an external antenna is normally more than one antenna connected. These readers are useful in applications where more antennas are needed, for example in a doorway.

5.3.1.2 Flexible reader

A type of reader that can read and interpret several different reader-tag protocols and data formats. This is done either automatically or by switching, but switching can influence the performance. To be able to read new standards, as they become available, the reader should be updateable.

This type of readers may be located at all entry and exit points in a facility. They can also be used on conveyors, at sort station or at any point where items must pass by. The benefit of a fixed RFID reader is its ability to automatically count and capture data, without the need of human involvement.

5.3.1.3 Multi-frequency reader

This reader can read both High Frequency (HF) and Ultra High Frequency (UHF) tags. Because of that is it unnecessary to buy, install and handle two different readers if both frequencies are used, they are on the other hand more expensive than readers with just one frequency. There is a need for this type of readers because there will never be one ideal frequency for all applications and protocols will not be simplified rapidly by the profusion of incompatible standards and proprietary technologies that are evolving.

5.3.1.4 Modular/interchangeable reader

A mobile reader can be moved throughout a facility, if it is located on a trolley or powered cart. Then the reader can be used to read all facility's contents economically. The big advantage with this device is that it can be a printer, reader and bar code scanner at the same time in an easily movable solution.

5.3.1.5 Handheld reader

For UHF, most handheld readers today are an own unit integrated to a portable computer. When it comes to Low Frequency (LF) and HF they can be like the ones for UHF, but normally it is just an own unit that does not need to be integrated in a portable computer. This reader is acceptable if only a few tags per read location need to be read at a time. They are also useful if the number of tags is too large for fixed location reader. The use of handheld readers is similar to using a bar code reader, but hand-held readers do not require the tag to be visible. There are currently no hand-held readers with a long battery life available and high power output. Because of the lower power output, compared with fixed-location readers, the hand-held reader has a shorter read range. You can clearly scan one pallet or case at a time, without interference from pallets close by, with a hand-held reader. That is the biggest advantage with this type of reader.

5.3.1.6 Label printer/encoder

This unit combines two key functions, printing standard barcode labels and encoding data into a passive RFID transponder embedded in the label.

5.3.2 Limitations of reader and tag communications

The science of radio frequency is analogue, not digital, and because of that is RF susceptible to degradation caused by interference from spurious RF sources and environmental conditions. The following examples can cause interference:

- Liquid, for example water.
- Metal, foil, or other metallic objects.
- High humidity.
- Extreme temperatures. Very cold or very hot.
- Motors and engines.

- Wireless devices, such as cell phones and Personal Digital Assistants (PDA).
- Wireless computer or communication network.
- Cordless phones.

How much these conditions affect a given RFID system's performance depends on the operating frequency. One of the most significant roles in the success of an RFID deployment is the capability to address interference issues. Because of that, it is critically important to extensive trials and pilots to enable optimal placement and installation of the individual RFID components. RF engineers are making great progress in designing systems to push the RF physics to overcome some of these limitations. At the same time, many of the inconsistencies and inaccuracies also can be addressed with sophisticated software solutions that implement error correction, fault tolerance and redundancy.

5.3.3 Anti-collision

5.3.3.1 Air interface

The air interface is the protocol that dictates how reader and tag talk to each other and make sure that the data avoid collision. The secret of the air interface is that a reader has a very specific way in which it encodes data by modulation. The tag can not communicate with the reader without knowing how the information from the reader is encoded. Most RFID anti-collision methods are time-domain

People did not begin to make bigger investments in the technology until well-accepted air interface protocol was designed. The modified Aloha slot protocol was finally chosen after years of deliberation. This is what you need to make sure that the tags you got will be compliant with EPC Generation 2.0 protocols.

5.3.3.2 Reader collision

One problem that can occur when you are using RFID is that the signal from one reader can interfere with the signal from another reader where coverage overlaps. This is called reader collision. To avoid this problem you can for example use the Time Division Multiple Access (TDMA) protocol. In simple terms, the readers are instructed to read at different times, instead of both trying to read at the same time. This instruction ensures that they do not interfere each other. But it means that each tag in the read range where two readers overlap will be read twice. The application software has to be set up so that if one reader reads the tag then the other reader will not.

5.3.4 Coding and modulation

5.3.4.1 Coding

Data transmission between a reader and the transponder in an RFID system requires three main function blocks, similarly to a digital communication system. From the reader to the transponder the direction of the data transmission is done.

These are signal coding and the modulator in the reader, the transmission medium, and the demodulator and signal decoding in the transponder. RFID systems normally use one of following coding procedures: NRZ, Manchester, UnipolarRZ, DBP, Miller and differential coding on PP coding.

5.3.4.2 Modulation

There are a lot of varied ways to modulate or altering the carriers to carry the encoded information. Different modulating techniques are in some cases used in each direction i.e. to and from tags. Modulation is a process in which the RFID tag changes the carrier signal of a reader to convey information. Radio technology is largely concerned with analogue modulation.
There are three different types of modulations.
Amplitude Modulation (AM), Frequency Modulation (FM) and Phase Modulation (PM).
These are the main variables of an electromagnetic wave. Other modulation procedures are derived from one of these types. In RFID digital modulation procedures are mainly used. Amplitude Shift Keying (ASK), Frequency Shift Keying (FSK) and Phase Shift Keying (PSK).
Other methods of modulating include Pulse Position Modulation (PPM), Pulse Duration Modulation (PDM) and Continuous Wave (CW).

5.3.5 The checksum procedure

When using data transfer with contact-less technology, it is very likely that interference will occur. Interference is causing undesired changes to the transferred data and thus is leading to transfer errors. To recognize transfer errors and initiate corrective measures, a checksum can be used. Parity checks, XOR sum, known as the LRC and CRC are the most common checksum procedures.

5.3.6 Interface between reader and software

Data exchange between the control unit and the software is performed by an RS232 or RS485 interface. Other interfaced used are Bluetooth, Ethernet (TCP/IP), WLAN and Zig Bee.

5.4 Antennas

5.4.1 Reader antenna

An antenna is connected to a reader (transceiver) and the antenna the sends out the reader’s signals. Basically, the reader tells the antennas how to generate the proper RF field. This field can cover an area from a few centimeters up to 30 meter or more. How large that area can be is depending on the power output and the frequency. When an RFID tag moves into the antenna’s radio field, it becomes activated. After the activation it sends back the information that is programmed into its memory. Through its array of antennas, the reader receives the tag’s signal and decodes the signal. The decoded signal is then sent to the software system. A reader can also transmit special signals to a tag, for example telling a tag to come alive, synchronizing a tag with the reader or interrogating all or part of the tag’s content. Antennas can act continuously or on demand. The continuously active system is used when tags are present regularly or for multiple tag reading in the antenna’s detection field. This detection field can be activated only when needed by a sensor of some kind and is called the on-demand method. Normally one to four antennas can be attached to one reader. There are some readers where up to eight antennas can be attached. (www.rfidconstructors.com)

From interviews we have found out that the use of several antennas can be necessary. The reason for that is the need of free sight when using frequencies in the UHF band to read on metal. With, for example, four antennas connected to a reader it is possible to cover a larger reading area from four directions. This is very useful, especially if the tagged items have different orientations in the reading area. An antenna gate can, for example, be used in a doorway or in the process line. It is important to choose the right type of antenna to a RFID system. Preferably the antenna should be a compromise between a very sharp tune, i.e. maximum performance without detuning, and a very flat tune that is less affected by detuning. (www.trenstar.com)
The following sections are discussing two important parameters to take into consideration when choosing reader antennas to your RFID system.

5.4.2 Polarization

Polarization is the direction of the electric field and is the same as the antenna’s physical configuration. An antenna in a RFID system can be linear or circular polarized. With linear means horizontal, vertical or any direction. Circular can be either right circulation or left circulation. In a simple way you can say that if your antenna is a dipole with linear polarization, it broadcasts out in a line that generates from that dipole with circular polarization the radiating signal spins
What type of polarization you use in your RFID system is an important factor, especially in determining the interrogation zone, range and accuracy of communication. A linear reader antenna offers a higher range that a circular reader antenna. There is normally no defined relation between the tag antenna and the reader antenna in an RFID system. This can lead to variations in the read range, which are large and unpredictable. By using a reader antenna with circular polarization, this problem can be solved. The problem with variations, using a linear antenna, is caused by the orientation of a tag’s antenna, with respect to the reader. Linear antenna is therefore more suitable for applications where the tag’s orientation always is the same, when it is placed on an item Today most antennas have circular polarization.

5.4.3 Directivity

The guiding parameter for point-to-point communication is the antenna property of directivity. In a wireless data network where you for example want to have connection between the reader antenna and the tag antenna, you want the signal to radiate in a preferred direction. If the signal radiates in other directions than preferred, other antennas can receive the data. When using antennas in RFID, it is preferable for the transmitted signal and the received signal to be confined in a specific area and not broadcast into other RFID zones or systems. Signals received from another RFID interrogation zone create so-called phantom reads or ghost reads. This can be a big problem, but can be helped with tests before implementing your FID system. The point of this section is that the system will work better the higher the directivity is.

5.5 Frequency ranges

5.5.1 125 kHz

This frequency is in the Low Frequency (LF) range and is the one used in Sweden. For man-years has RFID systems in the LF range been utilized in several industries? One of the biggest advantages with LF is that it is not as affected by surrounding metal. Therefore it is ideal to use for identifying metal items. Depending on which reader being used and the size of the transponder, the reading range varies. It can be from a few centimeters up to a couple of Meters. LF penetrates most materials, such as body tissue and water. One limitation is that electric motors may interfere with the LF system if it is used in the industry. Because of the antenna size, the LF transponders are normally more expensive than HF transponders. That makes this frequency best suitable for applications where the transponders can be re-used. Other limitations are that the data transfer is relatively slow, because the lower the frequency is the slower is the communication. One transponder at a time can be read in most LF systems and it does not support simultaneous read of multiple tags.

This frequency is used world-wide and there are no restrictions. Most access control systems are currently based on LF, key fob or contact-less cards for security. The automotive industry is the largest user for LF RFID systems. All car immobilizers (key) are using an LF transponder embedded into a car key with a reader mounted in the ignition. Parking lot and vehicle identification for highways are other applications that use LF systems. Around the reader antenna, the magnetic field is allowed to be 72 dBuA/m at 10 meters. If an external antenna is used a loop coil antenna may be employed.

5.5.2 13, 56 MHz

The frequency used for High Frequency (HF) RFID systems is 13, 56 MHz. This is a globally accepted frequency meaning that any system operating at HF can be used world-wide. There're still some differences with regulations in different regions of the world. They are primarily about bandwidth and power. HF is the basis of several standards, but they are discussed in the section Standards. When using HF, the signal travels well through most materials, even water and body tissue. Compared to LF, it is more affected by surrounding metals. The advantages with HF, when comparing to LF, are lower tag costs, the communication speed is better and it is possible to read multiple tags at once.

The antenna length is based on the length of the signal that are transmitted or received. You can say that the higher the frequency the shorter the wavelength is. Because of this, the antennas in a HF system are smaller than the ones used in a LF system. HF is designed for applications with that require a communication range of one meter or less, with the current power regulations. One thing that has an impact of the communication range is the orientation of the tags with respect to the reader antenna. Both the reader antenna and the tag antenna should be parallel to get the best communication range as possible. If the tag is perpendicular to the reader antenna, then the communication range may be reduced. (www.rmoroz.com)

In HF RFID systems, the communication range is highly dependent on the reader design and the transponder antenna. Parameters on which the maximum communication distance is depended are RF power of the reader and specific antenna configuration. Factors that strongly influence range are tag tuning, antenna size and environmental factors. The best communication range, in systems where only a single tag is likely to be in the RF field, is obtained by tuning the tag antenna for a resonant frequency equal to the carrier frequency of 13,56 MHz. If the tag is tuned to the carrier frequency, it can more easily extract sufficient power to operate, which maximizes the communication range.

To compensate for the detuning effect, if multiple tags are in the RF field at the same time, the resonant frequency should be higher than the carrier frequency. Due to the mutual inductance between the multiple tags, detuning causes the resonant frequency of each tag in the system to drop. The detuning effect can shift the resonant frequency more than 1 MHz.

A greater impact on the communication range, if comparing with tag tuning, has the relative size of tag and reader antennas. Tag antennas with larger diameter provide longer communication range when comparing to antenna with small loop antennas because they capture more current from the magnetic field. Larger antennas on the reader results generally in a longer communication range, but it is also possible to make the antenna too large. The tag may operate at long distance, if an antenna is too large, but not at a short range near the centre of the reader antenna. When readers are embedded in industrial or manufacturing equipment, the space for the antenna is restricted by construction of the equipment. In these applications, a small spiral antenna on the reader often provides the best range.

With 13, 56 MHz systems, water does not interfere, but metal does. If there are metal between the reader and the tag, communication is impossible. Even the thinnest metallic foil will short out the magnetic field from the reader. That will prevent the tag antenna to capture the current it needs to operate. Between the two antennas, the space must be clear of metallic materials. Tags can be embedded in plastic or epoxy with a minimal impact on range, because insulating materials do not interfere the magnetic field.

Another thing that can prevent the tag from communicating with the reader is to mount it directly on a metallic object. The field will be shorted out when metal is behind the tag antenna, just as it does in front of the antenna. To restore communication, the tag should be placed on an insulating spacer or ferrite spacer. A ferrite spacer must be used if mounting a reader antenna on a metal surface. No ferrite is necessary if the antenna is mounted above centimeter from the metal. Near the edge of the antenna, metal is less detrimental than if the metal is parallel with the antenna. If installed in the vicinity of metal, the reader antenna maybe re-tuned. (www.atmel.com)

With higher frequency the data throughput will be higher and the communications between readers and tags will be faster. This allows a reader to communicate with multiple tags at once. Communication with multiple tags is a process called anti-collision which is discussed in the reader section. A reader can read up to 50 tags per second when using HF. Tags in HF systems have larger memory capacity comparing to LF system tags. Normally should not electrical noise, which may be generated by motors in an industrial environment, affect a HF system.

Most access control systems today are based on LF, but HF is becoming technology of choice for new access control and security systems. Because of the larger memory capacity, HF systems allow for improved security. It also allows the integration of biometrics as part of the security features. Enhanced access control systems have the ability to validate assets, like computer equipment and other items as one passes through an access control system or portal. Within the access control system, assets embedded with a HF tags can be read and identified. Documents and files can also be easily identified and tracked. Several sports team and events are using HF systems in RFID applications for payment and access. Many ski hills in Europe use this technology for convenience and for prevention from fraud.

Normally a magnetic field in this frequency is allowed to be 42 dBuA/m at 10 meters. When using the frequency to RFID applications it is allowed with 60 dBuA/m at 10 meters for the magnetic field. (www.rmoroz.com)

5.5.3 868 MHz

This is a frequency in the Ultra High Frequency range (UHF) and is the one of two frequencies used in Sweden for UHF RFID systems. The other frequency used is 2, 45 GHz that is discussed in the next section. Lately, this frequency has become one of the dominating in RFID market space. The reason for this is the EPC standard that is discussed in the section Standards.

One of the biggest reasons why UHF has become more popular is the read range. Even if LF and HF are well-established and robust technologies, they fail where range of beyond one meter read is required. On the supply chain market where longer read distances are required, UHF systems are preferable.

RFID in the UHF range differs from HF systems in many ways. UHF range allows for shorter antennas and longer read distances. Reader-tag communication is implements that often are using back- scatter technology. This method is described in the section communicating principles.

In UHF, the anti collision feature implementation is achieved using a protocol based on bit broadcasting. A higher number of tags can be read simultaneously because of the use of this protocol. It is possible to read about 200 tags at once with UHF in RFID systems.

Today's UHF systems do not work in presence of liquids and on metal poses it is normally a serious challenge. Another disadvantage, caused by the longer read range, is applications like banking and access control. One problem with UHF is that it uses different frequencies indifferent regions of the world. In North America, UHF operates at 902. 928 MHz, in Europe, UHF works in the 860. 868 MHz range and Japan uses 950. 956 MHz. (www.rmoroz.com)

When using UHF radio waves will bounce off metal. For that reason it is necessary with a small space between the item and the tag. The normal solution has been to use some sort of spacer to lift the tag of the metal. This spacer is usually thick and can cause the tag to be knocked of the object with slight contact. One company has developed a line of thin isolator material, which is substantially thinner than the usual spacers have and enables the RFID tag to be read on metal while maintaining a low profile. (www.eccosorb.com)

When metallic are close to the tag's antenna or the reader's antenna, a change in the characteristics of the system will occur. For the antenna on HF and UHF tags, metal changes the inductance of the antenna and basically re-tunes its resonant frequency. Because of that will the overall read range be reduced. (www.packagingdigest.com)

Signal attenuation

In RFID, attenuation normally refers to reduction in the energy that is emitted by the reader or in the energy reflected back from the tag. A tag must be closer to the reader to be read if less energy is able to reach it. The energy emitted by the reader is naturally decreasing with distance. This rate of decrease is proportional to the inverse square of the distance. Passive UHF-tags reflect back a signal at very low power levels.

By the way a system is installed or external factors, such as the items tagged, can also cause signal attenuation. Many readers have one or more external antennas that emit radio waves. These are connected to the reader by coaxial cables. Placing reader antennas too far from the reader can cause poor performance. The reason to that is as the energy travels from the reader, through the cable, to the reader antenna, the signal attenuates. (www.absoluteitsolutions.com)

Electromagnetic interference

EMI is most of all noise that makes the possibility to get a clear signal back from the UHF-tag harder. A wide variety of machines can cause this type of noise. Motors emit EMI and may need to be shielded to prevent interference with RFID systems. On manufacturing lines, most robots cause interference and so do conveyors with nylon belt. (www.absoluteitsolutions.com)

In Sweden, a reader antenna in this frequency range is allowed to send out an effect of 2 W Effective Radiated Power (erp) and that has been in law since 1 January 2006. Other regions of the world usually allow higher radiated effect, for example in USA it is 4 W Effective Isotropic Radiated Power (eirp). The reason for that a higher radiation allowed in this frequency range is EPC. This is discussed more in the section Standards. The difference between erp and erp is what the antenna gain is relative to, for erp it is a half-wave dipole in a given direction and for eirp it is an isotropic source. (www.epcglobalinc.org)

How much effect the reader antenna is allowed to radiate affects the read range. With a higher radiated effect, the read range will increase.

5.5.4 2, 45 GHz

The frequency 2, 45 GHz is also called microwaves. This frequency ranges are from 1 GHz and upward. For RFID systems, a typical microwave operates either at 2, 45 GHz or 5, 8 GHz; in Sweden the former one is used. Microwave systems can use both semi-active and passive tags. One great advantage is that these systems have the fastest data transfer rate between the reader and the tag. Because it is in the UHF band, microwaves got the same drawback when
Using it in presence of metal or water, as 868 MHz. (www.informit.com)

The antenna length is inversely proportional to the frequency and because of that the passive tag's antenna has the smallest length comparing to the other frequencies discussed. That makes tags in microwave RFID systems, the ones with smallest size. Another reason for the small size is that the tag microchip can also be very small.

The 2.45 GHz frequency range is called Industry, Scientific, and Medical (ISM) band and is accepted world-wide. For this frequency range, the reader antenna is allowed to radiate with 0, 5 W eirp in Sweden. Power levels above 0, 5 W are restricted to use inside boundaries of a building and the duty cycle shall in this case be <= 15 % in any 200 ms period, 30 ms on/170 ms off.

5.5.4.1 Surface Acoustic Wave (SAW)

An interesting part of UHF 2, 45 GHz is the SAW technology, which is based on chip less tags. These tags are passive and offer a large read range, approximately 10 meters. The chip used for SAW tags normally have a low cost and they have a small antenna. For temperatures up to 400 degrees Celsius can these tags survive, but not in acids.
Since the tags are simple, all functions, such as anti-collision, have to be in the reader unit. SAW technology also offer a high-speed reading. (www.rfsaw.com)

5.6 Communication between tag and reader

To read from or to write to the transponder it must be possible to transfer energy and data between the tag and the reader. There are three main procedures to achieve this transfer, Full Duplex (FDX), Half Duplex (HDX) and Sequential transfer (SEQ). In the full and half duplex procedure the energy is transferred continuously, but for the sequential procedure the energy is transferred under a short period of time. Sequential systems are often called pulsed systems.

5.7 Communicating principles

The data and energy transmits between the reader and the transponder in a few different ways, inductive coupling, electric backscatter coupling, close coupling and electrical coupling. Depending on which frequency is used the different coupling methods are using the electric, magnetic or electromagnetic field. The ranges for the different coupling is between a few centimeters, close coupling, up to over hundred meters, active backscatter coupling.(

5.7.1 Power transfer

When we are discussing power transfer between the reader and the tag we, of course, mean between a reader and a passive tag. The active and semi-active tags have their own power sources i.e. battery.

´

5.7.1.1 Inductive coupling

An inductively tag compromise of a chip, to store information, and a large area coil that functions as an antenna. Because most of the inductively coupled systems are passive, the tag needs to take all energy that is needed to operate the chip from the reader. To provide the tag with all that energy that is needed the reader creates a strong electromagnetic field. Because of the long wavelengths, often many times the distance of a normal RFID system, of the frequencies that are using inductive coupling, 2400 meters for 125 kHz and 22, 1 meter for13, 56 MHz, the electromagnetic field can be treated as a magnetic field. This magnetic field only exists in the near field of an antenna; the near field exists approximately up to a half wave length from the antenna. This means that inductive coupling only are used for lower frequencies, LF and HF. A small part of the magnetic field that the reader creates penetrates the tag antenna coil and induces a voltage in the tag antenna coil. The antenna coil of the transponder and the capacitor, form a resonant circuit which has its resonant frequency tuned to the reader's transmission frequency. When a tag frequency corresponds with a reader's frequency the voltage reaches its maximum. This voltage is rectified and are used a power supply to the chip. The efficiency of power that are transmitted between the reader and the tag is proportional to the frequency, the number of windings in the coil, the area that the coil encloses, the angle of the two coils relative to each other and the distance between the two coils. This means that with increasing frequency you can have fewer windings and still have the same efficiency, 125 kHz has typically 100-1000 windings and 13, and 56 MHz has typically 3-10 windings.

5.7.1.2 Electromagnetic backscatter coupling

RFID systems that have a distance between the reader and the tag that exceeds one meter are called long-range system. These systems are operated at UHF, 868 MHz, and microwave, 2, 45 GHz, frequencies. The short wavelengths of these frequencies, 12 centimeters for2,45 GHz and 35 centimeters for 868 MHz, means that the transponder antenna becomes much smaller and more effective than for the lower frequency ranges. The power that the chip needs to operate is induced in the tag antenna as for a normal antenna, dipole or other. If the transponder is an active transponder the energy induced in the antenna is used as a wake-up signal.

5.7.1.3 Close coupling

Close coupling systems are designed for very short ranges, 0, 1 centimeter up to 1 centimeter. This means that the transponder have to be inserted or be placed on the reader. When the tag is inserted, or placed on, the reader it will be positioned in the air gap of a ring shaped or U shaped core. The function of the close coupling systems is like that of a transformer where the reader represents the primary winding and the transponder represents the secondary winding. A high frequency alternating current in the primary winding generates a high frequency magnetic field in the core and air gap between the tag and the reader. This magnetic field flows through the transponder coil and induces a voltage in the coil that rectified and used to supply the chip with power. Close coupling system has very high efficiency when it comes to transfer power, in contrast to inductive coupling. This means that close coupling is well suited for systems that contain tags with high power consumption.

5.7.1.4 Electrical coupling

In an electrically coupled system the reader generates an electrical field which is used to transfer the power over to the tag. The antenna of the reader often consists of a large metal plate or metal foil. When a high frequency voltage is applied to the antenna an electric field between the antenna and ground is formed. The antenna of the tag is made by two conductive surfaces lying in a plane with the chip lying in between. When the transponder is placed in the interrogation zone of a reader, in the electric field, an electric voltage rises between the two conductive surfaces and supplies the chip with power.

5.7.2 Data transfer

Here will we discuss the transfer of data from the transponder to the reader. Data transfer from the reader to the transponder will be discussed elsewhere.

5.7.2.1 Inductive coupling

Load modulation

As long as the tag, in an inductive coupled system, stays in the near field the system will act as a transformer system with the reader as the primary coil and the transponder as the secondary coil. The tag will draw energy from the magnetic field. The transponder will then transfer its data content to the reader. This data transfer is achieved by switching a load resistor, or capacitance, on and off at the tags antenna. By switching the load resistor the impedance of the transponder will be changed and the voltage at the antenna will be changed as well, this is a way of achieving an amplitude modulation. If the data stream controls the switching of the load resistor the data can be transferred to the reader. This is called Ohmicload modulation. If we instead have a capacitor that we switch on and off, we will change the resonant frequency of the tag between two different frequencies. This will generate a combination of amplitude and phase modulation. This is called capacitive load modulation.

Load modulation with sub carrier

Load modulation is also performed with a sub carrier, instead of switch the load resistor on and off in time with the baseband-coded signal, a low frequency sub carrier f_s is created by binary division of the operating frequency. This creates two sidebands to the baseband that is located ± f_s from the baseband. This sub carrier is modulated by the baseband by ASK, FSK or PSK and used to switch the load resistor on and off.

Sub harmonic transfer

Another way of transmitting the data from the tag to the reader in an inductive system is to use a modulated sub harmonic. Division of the reader frequency, often division by two, creates a secondary frequency, sub harmonic. The output from the divider is then modulated with the data stream from the chip and fed into the transponder antenna via an output driver.

Electromagnetic backscatter coupling

The principle for backscatter coupling is based, as for radar, on reflection of radio waves. The reader transmits a radio wave to the tag; a small proportion of the incoming power is reflected back from the tag antenna out into space. Altering a load connected to the antenna can vary the amount of power that is being reflected from the tag. To transmit data from the transponder to the reader a load resistor is connected in parallel with the antenna, the data stream from the chip switches the resistor on and off. The switching of the resistor varies the amplitude of the power that is reflected from the tag that the reader antenna picks up and demodulates in order to receive the information. To switch the resistor on and off a FET transistor is used .

5.7.2.2 Close coupling

Closed-coupled system with magnetic data transfer between the transponder and the reader is using load modulation with sub carrier to transmit the data. Some closed-coupled system uses capacitive coupling for data transmission between the transponder and reader. In capacitive coupling the capacitors are constructed from coupling surfaces isolated from one another. When the tag is placed inside the reader the capacitors are placed exactly parallel to one other and the data can be transferred.

5.7.2.3 Electrical coupling

When an electrically coupled transponder is placed in the interrogation zone of a reader, the input resistance of the transponder acts upon the resonant circuit of the reader via the coupling capacitance between the reader and transponder. This damps the resonant circuit slightly. This damping can be switched between two different values by using a modulation resistor. Switching the resistor on and off changes the resonant circuit and therefore changes the amplitude of the voltage that is present at the reader. By switching the modulation resistor we can send data from the tag to the reader.

5.8 Standards

There are no existing standards for RFID today; the standards that exist today are only for very specific applications. This means that every manufacturer has his own standard, so the readers from Texas Instruments can not read tags from Philips. There is however readers that can read tags from more than one manufacturer. The closest thing that can be called a standard is EPC, Electronic Product Code. More and more big retailers, like Wal-Mart (US) and Metro (D), are supporting EPC. But EPC only has standards for 868 MHz, in Sweden, and is voluntary. There are some standards that exist but they are only for some very specific application such as Animal Identification and Smart Cards, which require encryption to maintain safe data transfer. There are some other standards on its way, like tracking goods with HF or UHF transponders. www.rfidjournal.com)

5.8.1 International Organization for Standardization (ISO)

ISO is the largest developer of technical standards in the world. ISO is a network of the national standards institutes of 156 countries with its central Secretariat in Geneva, Switzerland. (www.iso.org)

There are a few standards for RFID that ISO has established.

ISO 11784, 11785 and 14223 are standards for identification of animals using RFID.

ISO 10536, 14443, 15693 are standards for Smart Cards.

18000-1. 10000-6 are ISO standards for Air Interface Communication for the different RFID frequencies.

5.8.2 Electronic Product Code (EPC)

EPC global is the organization that has established and is supporting the EPC global Network as a standard for real-time, automatic identification of information in the supply chain. EPC global has standards for 13, 56 MHz and 865-930 MHz. EPC global specifies technical protocol that defines how the data is structured on the tag and communicated between tag and reader. (www.epcglobalinc.org)

For Sweden there is only one frequency that EPC has standards for and that is the865-868 MHz. And in mars 2006 the EPC Class 1 Generation 2 was adapted to ISO 18000-6as an international standard. (www.gs1.se)

EPC Class 1 Generation 2 is passive backscatter tags with 96 bits of memory. It has to be a WORM tag with a Kill command that permanently disables the tag. (www.epcglobalinc.org)

EPC has six different classes, that defines which type of tag, if the tag has a power source or not and how much memory the tag has. (www.epcglobalinc.org) The bit structure of an EPC tag consists of an fix length header followed by a series of numeric fields whose length, identity and structure totally depends on the header value. (EPC global tag data standard version 1.3, 2006)

Header

As we said before, the header defines the structure, length and identity of the EPC code on the tag. The header always consists of 8 bits and the value 11111111 is reserved for future expansion of the header space. (EPC global tag data standard version 1.3, 2006)

EPC Class Definition

Class 0 RO passive tag
Class 1 WORM passive tag
Class 2 RW passive tag
Class 3 Semi-active tag
Class 4 Active tag
Class 5 Reader

Header EPC Manager Number
Object Class Serial Number
8 bits 28 bits 24 bits 36 Bits
0011 0101 Binary number
268 435 455 Max decimal value
16 777 215 Max decimal value
68 719 476 735 Max decimal value

EPC Manager Number

The EPC Manager Number identifies a company, organization or manager that is responsible for maintaining numbers in the Object Class and Serial number fields. EPC global assigns the EPC Manager Number that will ensure the uniqueness of the entity that uses EPC tags. (EPC global tag data standard version 1.3, 2006)

Object Class

The Object Class is used by the EPC managing entity and identifies a class or group of things. The Object Class number must be unique for within every EPC Manager Number domain. (EPC global tag data standard version 1.3, 2006)

Serial Number

The serial Number must be unique within each Object Class. The serial Number is used for identification of each individual of every Object Class. (EPC global tag data standard version 1.3, 2006)

5.8.3 European Telecommunications Standards Institute (ETSI)

ETSI's mission is to produce standards for telecommunication. ETSI is a non-profit organisation with 654 members from 59 different countries. ETSI EN 302 208 is a standard for the 865. 868 MHz and defines for example how much power the reader may transmit. (ETSI TR 102 436v1.1.1, 2005)

6 Security

As in terms of organization or the business is concerned the security is looked as one of the major issue which most of the organizations face. Organizations have defined policies and procedures which must be confined while implementing the RFID solutions for any process within the organization. This need to be done in a structured approach.

In the following paragraphs we will be dealing with both problems but with more emphasis on data security which is in term main focus of this thesis.

6.1.1 Privacy

Privacy is increasingly under threat from all kind of sources today. We have increasing numbers of CCTV cameras in the cities monitoring every our move, mobile phones eavesdropping, e-mail control and all kind of computer monitoring and surveillance. These and many other ways of intruding on our privacy today are leading to the feeling that we are not alone and safe even in our own houses. RFID and especially EPC's uniquely identifiable products concern and worry many people who believe that this technology will just add more pressure on individual privacy.

The possibility that a business could loose control of the privacy of its information is one of the largest risks associated with RFID. For example, the potential exists for tag "sniffing" of a running production line from the parking lot. Like Ethernet networks, wireless tag communications are subject to capture and analysis. With all but the strongest data security algorithms subject to successful brute-force cracking using portable or networked computing resources, the cryptographic capabilities of tags becomes an important consideration in their selection. The information inside RFID tags is vulnerable to alteration, corruption and deletion. The first question to be answered is how vulnerable the tag data is. Tag security can be expressed in terms of the strength of the cryptography employed, the processing speed of the tag and the amount of time it takes to establish a secure channel of communication with that tag. Compromising the security techniques employed in an effort to reduce tag complexity—and cost—yields tags whose mean time to "crack" is measured in mere minutes. The security of information between RFID tags and readers is only now being strengthened to meet commercial needs with Gen 2 tags. Tags that present surmountable barriers for compromise represent a potential supply chain disruption opportunity. In the extreme, such disruptions might include the purposeful re-programming of tags to reflect errant weight, quantity or size information. Companies that select a weakly secured tag give competitors a low-cost opportunity to passively gain details about their suppliers, quantities on-hand, inventory turns, shifts in product mix and product destinations (customers).

6.1.2 Data Security

Data security is a second important issue that needs to be explained when we talk about RFID's security and is equally if not more important than privacy concerns. This issue is much more important for the research goals of this thesis and thus it will be dealt in more detail. RFID's potential wide spread implementation in systems like authorized facility access, toll payment, retail, supply chains and many others, will with it necessary bring attempts to misuse and tamper with technology. These attempted attacks may range from very innocent just plying with the technology ones, to cases of corporate espionage, forgery and theft. According to RFID Journal there are three primary issues surrounding
RFID and the need to protect proprietary information:

Protecting data stored on the tag;
Protecting the integrity of the tag (and thus the product);
Securing data related to the serial number on a tag, which may be stored in a network database.

None of these issues are impossible to overcome, but they require companies to make some tradeoffs, and the only way to make the right decisions is to understand the options available. Let's revise all three in more detail.

Protecting data stored on the tag
When dealing with this issue there are three main situations that need consideration, the first is preventing someone from reading the tag, the second is preventing someone from changing the data on the tag and the third is preventing someone from eavesdropping on the communication between the tags and readers.
Even though it might seam that somebody's unauthorized reading of the RFID tag is not a 'big deal' it can actually present a great problem. Reading a single tag from a product like shampoo basically presents very little danger, the only thing that trespasser can obtain is ISO or EPC serial number of that product and maybe some additional information about the product (e.g. country of origin, expiration date, etc.). This amount of information seems insignificant and for a layman it is hard to imagine any situation where this information could be misused. Now let's imagine that your competitor has noticed that your supply chain is more cost effective and/or that you acquire your products at much lower prices than he can. Normally it would take him certain amount of resources and time and some corporate espionage in order to find out reasons for your sources. That was in the pre RFID era, now the only thing that he needs to do, if your tags aren't protected, is to reed one and he has all the info that he needs to discover your little secret.
Solution to the problem in this particular situation might be that you would not keep this info on the tag it self, instead you would store it in a database where it is only accessible to you, or you could encrypt the data and make it unreadable, but about that and other protection methods will be more talk later in this paper.

Our next worry is, if somebody can read one of the tags he can probably read all of the tags with the same level of protection. Again previously mentioned scenario is a possibility, but even if we combat it, with not storing anything except the identity code on the tag it self we are still facing significant problem. The same technology (RFID) that makes it easy for us to keep track of our products and view real time inventories is also making those things possible for others. So if our tags are unprotected our competitors or anybody else with enough technology in his hands can keep track of our supply chain and the goods flow. All that data can provide them with very useful facts about our business; where we buy our raw materials, where we ship them, how much we ship, how much we sell, consequently how much we earn and much more. Information like that in wrong hands can be very harmful for the unsuspected victim. Again this problem can be solved with some protection measures like encryption but more about it in the encryption section of this chapter. Second thing that should be on every RFID's professional mind, when thinking about data protection, is that there are ways and methods that allow unauthorized change of the data on the tag, in case of rewritable tags. One of the tools that ill intended person can use to tamper with the data on the tag is a software program called RFDump. This tool is one of the famous ones but most definitely not the only tool or the only way to manipulate tag data. The RFDump software allows to a user equipped with an RFID reader, a laptop or PDA, and a power supply to rewrite the data stored in ISO 15693 tags, the most common tags used to host the EPC (Electronic Product Code) information traditionally stored in bar codes . With this kind of tools data is very vulnerable if it is not protected by some sort of software or mechanical protection. Consequences of this kind of shortcoming can be very grave. Situation that could then occur is that thief could change the identity of the product, making a very expensive stereo read as a cheap Walkman at the automated cash register at the exit of some retail store. Even worse scenario could be if you have a container full of goods intended for your warehouse and on its route a skilled port worker, where your container is offloaded, changes your data on the tag with data from some bogus company that his criminal organization established. Then instead of delivering that container to you it will be delivered straight to the thieves. The second scenario is less likely to happen because systems that handle containers are still not as highly automated as retail industry soon will be and the RFID technology used on containers is much tougher to tamper with. Even though at the moment container theft as described above is not an easy task, items like containers and expensive goods are in greater danger form data changing attacks than retail (cheaper) goods. Main reasons for that are their great value and the fact that they use more expensive re-writeable tags that can then be reprogrammed, on the other hand in retail ''when RFID tags are eventually placed on individual items in stores, companies will almost certainly use low-cost, read-only tags''

The third issue, in tag data protection sphere, is preventing someone from eavesdropping on the communication between the tags and readers.

The presumed problem here is that if someone can tap in on the communication, he can gain valuable information about the tag, data on it, encryption methods and/or the reader. All that info can later be used for unauthorized access to the tag, identity theft (substituting identity codes on products), tampering with the data or some other forms of malicious wrongdoing.

Although readers may only read tags from within the short tag operating range (e.g. 3 meter), the reader-to-tag, or forward channel is assumed to be broadcast with a signal strong enough to monitor from long range, perhaps 100 meters. The tag-to-reader or backward channel is relatively much weaker, and may only be monitored by eavesdroppers within the tag's shorter operating range. Generally, it will be assumed that eavesdroppers may only monitor the forward channel without detection.

One of the solutions to this shortcoming, which is suggested by Auto-ID Centre is to limit the number of times when reader broadcasts an ID number to the tag. The reader can, for example, break up the serial number and only broadcast a part of it. The tags that have the same part of the serial number respond, but this time with the full number. This way full number is only sent in the reverse channel, which is a whisper, compared to the forward channel, which is by necessity a lot louder. By doing this the probability that an eavesdropper will obtain complete serial number is reduced significantly. Another solution is to encrypt communication reader-to-tag and the other way round.

Protecting the integrity of the tag

When all considerations about data on the tag and access to it are settled, the next step is to think about tag integrity. Physical protection of both goods and systems predecessors of RFID was a problem that companies had to deal with for years, even before RFID. Even though this has been with us for so many years, it still inflicts great damage. Possible bad case scenarios with this issue are physical removal/damaging of the tag and 'killing' of the tag.' The Auto-ID Center's Class 0 and Class 1 specifications include a kill command that enables retailers to permanently deactivate the tag at a consumer's request. Some authors believe that the kill command has a serious drawback -- it creates a backdoor that those with ill intent could use to circumvent the system. If you can kill the tag in the packaging, then you might be able to put another tag on, with a phony serial number and get a high-priced item for a lower price'', but RFID technology it self is much more complex and harder to clone or fake than bar codes so it should improve integrity of data and products. Unauthorized killing can, according to Tom Pounds form Alien Technology, be prevented by having secret kill code that reader needs to send to the tag in order to kill it. www.savi.com

Physical removal of the tag, which can then be replaced with a fake one, is especially worrying for expensive goods retailers and other supply chain participants. Putting the fake tag on a single product or a container full of products allows the perpetrator to claim the goods as his own or simply fill his tag with data from some cheaper product and then buying the product/s much cheaper. This problem can be avoided by requesting authorization before killing order is accepted or not including the kill option in the first place. Another indirect damage is that if the tag is just damaged and the product it self is not actually taken, than the shelf space is occupied while your system says its not. This results in over ordering thus high inventory, lost revenues from not selling the damaged tag product, expenses for replacement of the tag. This problem can be devastating for container or that kind of voluminous shipments in the systems that rely to much on automation because than shipments can get stuck or even lost in the supply chain and that is exactly opposite of what RFID is supposed to do.

This can be combated in cheaper retail products with pressure sensitive labels, which prevent consumers from switching tags, or with some, more sophisticated methods when considering goods that are more expensive or containers/pallets. These sophisticated methods include tags that would react when tampered with and notify the owner, or making them part of the product. So far we were talking about preventing others from reading the tags, from eavesdropping on communication, from reprogramming the tags, or obtaining access to our data bases, now we need to see how RFID can helping century’s old problem, physical theft. In almost all organizations main cargo loads are shipped in containers or some other sort of boxes and in the process they are opened and tempered with. To prevent this, seals with passive RFID tags (i.e. e-seals) can be placed on the goods or the box at the points where they could be opened. The reader then will be able to read data from the seals at regular intervals to detect when a shipment has been tampered with. The e-seals can be in the form of a sensor bolt or smart seal with an embedded RFID tag that is used to lock the container doors and also monitor any tampering with the container door lock or even monitor things like change in temperature, humidity and shock. There are currently more than 16 million shipping containers in use around the world, and seals are used not necessarily to prevent access, but just record if tampering took place .In this case, RFID tag is inside the container or another packaging and thus it is very hard to physically tamper with it, which makes it very secure. On the other hand, if the tag is on the outside, like inmost retail products, tags can be made with a proprietary cushioned material that is laminated to printable labels, which enables a transponder's silicon chip and copper antenna to survive typical environmental hazards. Besides providing physical protection, the cushiony layer could also dissipate potentially damaging static electricity

Securing data related to the serial number on a tag, which may be stored in a network database

One of the solutions to a problem of unauthorized data reading from the tag, as mentioned before, is to keep the information related to the product not on the tag it self but in some sort of database. This database is then connected through Internet or intranet to the readers or other devices that need access to it. Data that is stored in this database can range from usual product specifications to encryption algorithms or keys used on specific tags,' killing' codes and other. In systems that Auto-ID Center specifies to use together with their EPC technology, databases with network capabilities have crucial part and thus these systems are much more vulnerable to this problem than systems with less critical database like most other systems are. Most problems that could occur in this perspective are very familiar to IT experts because they are dealing with them regularly in network-databases environment that doesn't necessarily need to be RFID related (e.g. financial service industry with its databases). The most highlighted problem is that off unauthorized access to the data in the database. Solution to this and other problems that might occur is access to the database on the need to know basis. Sanjay Sarma of Auto-ID Center says "You absolutely will need to use some kind of access control to make sure that someone who is not authorized can't get into the database". So it is crucial to determine who can access the data and when, which is determined by the company and then it is up to IT technology and experts to keep everybody else away.

6.1.3 Encryption

Encryption is a very important for this topic and for the research because it is the most used method of protection and it still has by far the best price to effectiveness ratio. ''When selecting a suitable RFID system, consideration should be given to crypto-logical functions. Applications that do not require a security function (e.g. industrial automation, tool recognition) would be made unnecessarily expensive by the incorporation of crypto logical procedures. On the other hand, in high security applications (e.g. ticketing, payment systems) the omission of crypto logical procedures can be a very expensive oversight if manipulated transponders are used to gain access to services without authorization'' . As we were mentioning before many unwanted situations can be avoided by having proper encryption method in place. In addition, as we have already explained the situations them self and the possible consequences, this part will then concentrate on different methods of encryption and benefits vs. shortcomings. names three types of cryptography that can be used to protect RFID; mutual symmetrical authentication, authentication using derived keys and encrypted data transfer (it needs to be said that these are certainly not the only cryptography methods available or in use).Mutual authentication between reader and transponder is based upon the principle of three-pass mutual authentication in accordance with ISO9798-2, in which both participants in the communication check the other party's knowledge of a secret (secret crypto logical key). In this procedure, all the transponders and receivers that form part of an application are in possession of the same secret crypto logical key (symmetrical procedure). If this type of protection is used with great number of transponders (tags), according to, there is a danger of perpetrator discovering the crypto logical key. That would be possible because all transponders included in this kind of system would have the same key and thus the key would be widely accessible to people involved with the system. If the key is discovered the whole system would then be exposed. Second type of cryptography, authentication using derived keys, solves this problem of wide accessibility, of one universal key by assigning specific key to each transponder. In this way, even if one key is broken the system is not in jeopardy.

Third type of cryptography, encrypted data transfer, is important when protecting against eavesdropping. First two systems were mainly concentrated on limiting access to the tag information to the key holder. Encrypted data transfer is used to make 'conversation' between reader and the tag non-understandable to unwanted 'listeners'.

Asymmetric-key cryptography or public key cryptography is also widely used cryptographic method with possible application in RFID. Public-key cryptography is a system that uses two keys; a public key, known to everyone, and a private or secret key, known only to the recipient of the message. An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key.
Typically, public-key techniques are much more computationally intensive than symmetric cryptography
With RFID, these public key schemes have traditionally been impractical to implement. Without a processor on the chip, it is difficult to do dynamic encryption, where the algorithm generates a unique key for each session, or where the key can change by session. For devices without a processor and in particular passive devices (those without a battery), such complex computations, (including encryption, decryption, signature and verification) are just too slow and cumbersome

7 Problems with security in practice

Most publicized and financially biggest projects related to implementation of RFID so far have been in retail industry. Here we have big corporations like Wal-Mart, Target, Metro, Gillette and Procter & Gamble introducing pilot projects or demanding from their suppliers and partners to adopt RFID in the near future. The rest of the implementation attempts in organizations until now have followed the principle of doing a small pilot project or just partially implementing the technology and avoiding full scale asset dedication and full system implementation. There are several reasons for applying this kind of caution but they are of no importance for this research. What is important for this research is that because implementation, thus usage, of RFID is still on relatively small scale problems with security that are experienced in practice by early adopters are also small scale and are far from their full potential. That is also one of the reasons why security is still lacking behind and needs to catch up with other issues related to RFID technology.

Problems named below are already happening or are most likely to happen in practical application of RFID due to technological and other shortcomings named before. Other important thing to mention is that these problems were also named for their great potential for causing damage to RFID supply chains. Even though RFID systems are not fully in place, yet the problems are already occurring and sending ominous warnings for the future. One of the problems encountered in existing RFID projects was a possibility for unauthorized reading and in some cases even changing the data on the tags. Reading of the tags was possible with almost all of the tags used in retail because the level of protection they used was low or in most cases nonexistent due to tags low cost requirements. By the time this report was written to the authors knowledge there were no harmful exploitation's of this shortcoming in it self, but in combination with tags that allowed changing of the data there were some incidents where fraud or theft were involved (or at least proven possible). In this respect we have a case at Metro future store where Lukas Grunewald, the German consultant, claims that he, with a use of some hardware and his own software RFDump, managed to change the data on the individual product tag and thus factually breached security and made it very easy to defraud Metro by paying for the product below its original price.

Throughout the different processes, when it becomes RFID enabled, there will be opportunities for unauthorized data gathering. When using current technology this presents one of the most probable and thus most dangerous types of security breach. The part of the processes when goods are being distributed is one of the most dangerous parts and it is the time when system is most exposed to unwanted attention. Your competitors or basically anybody equipped and skilled enough to operate a few readers and a PC will be able to track and trace your goods as good as you can. For some this presents no danger because sharing info is something they already do or it is not damaging to them to allow it anyway, but for most keeping their business to them self is one of the basic business premises. In majority of situations, this can be avoided if good enough encryption is in place or if tags are shielded from unwanted reading during their movement throe the supply chain. Pete Abell, an RFID consultant at Boston-based EPC Group, says that as stores adopt the technology beyond the test phase, any shopper who brought his own RFID reader into a store would likely bedetected[38]. Well maybe not. Current commercial readers are big and cumbersome thus easily detectable, but when ill intended person makes one for the sole purpose of misusing it, that reader can be hidden much better and definitely smaller, even more so with technology progress. Other problems that could occur in near future, when implementation of RFID gets on its way, include but are not limited to: denial of service, tag removal/replacement, data bases attacks, large scale unauthorized tag readings, and RFID enabled theft and fraud. All these problems have been explained in more detail in previous chapter so here they are just named.

Experiences and practices accomplished so far, in the respect of Security in pilot projects and small scale application, should not be taken as very reliable and as appropriate measure for future use, main reason being that when implementation scales increases, risks and threats increase significantly and even some new and earlier unforeseen emerge.

Let’s now proceed to see which of those problems are more likely to occur and how important each of them is to be dealt with.

8 Relevance and importance of different problems

As mentioned number of times previously we can only predict, with more or less success, what will actually happen with RFID systems and their security? Keeping that in mind is essential when determining how these problems relate to each other and the system it self according to their importance. In a context we look at importance of each potential problem according to how significant is the damage it can case and how probable is it to happen. In previous section of this chapter, we have introduced the possibility of unauthorized data gathering with the help of RFID technology and now we name it here because it presents the greatest and most probable threat in the near future. Not everybody will agree with this statement, some other threats may seam much more dangerous for them, but because of the stage of the development of RFID and the ways early adopters are planning to use it, other security threats cannot compare yet. The strong emphasis is on yet. Future technological advancements and continued spread of RFID usage will possibly shift this balance to some other threats. Significance of this problem may not be apparent immediately, but because it is technically very easily accomplished and possible ways to misuse gained data are numerous it means that it is highly probable and potentially very damaging in comparison with other potential threats. Second very damaging and highly probable security problem is denial of service attack. This problem can be divided in two different ways it can occur. One is when your reader-to-tag communication is being interrupted and the other is when IT part of your RFID system is being attacked in order to disable it and deny you the use of it. It has to be said that immediate damage caused by this attack can be devastating but because it is much less probable and significantly harder to perform than the data gathering, it is mentioned as second most important. Another problem that can occur and cause significant damage especially in current highly unsecured RFID systems is accessing and changing data on the tag. A successful tag data changing can result in attackers getting products cheaper, confusing system (causing you problems with tracking, tracing or inventory management) and stealing. There are of course more damaging possibilities for this kind of threat but they are less likely to occur and less damaging so they won't be discussed here. This threats occurrence probability and for that mater damage sustained by RFID systems can increase in future highly automated systems if insufficient protection or control systems are not in place. Majority of the systems implemented with RFID is still far from being fully automated and it is likely they are going to stay like that for some time in near future. Damaging and/or removing the tag from the goods is similar to a problem that was faced with barcode technology while its significance and potential damage that it can cause in RFID enabled environments, is much greater than it ever was with barcode. Importance of this problem again increases in relation to the level of automation applied in the system. The more computers involved the greater the danger of it occurring and greater the potential damage. If this kind of threat is considered in retail environment, where you have tags on single products, potential damage is significantly lower than if you consider container or pallet size shipments in distribution channels. The focus here is more on deliberate then on the accidental damaging of the tag and by damaging it is meant rendering the tag unusable.

Here we again come back to the fact that RFID still isn’t being used to its full potential and thus security now and when RFID reaches its full potential may differ significantly. Depending on situation, level of RFID integration and implementation, this importance rating can vary. These are major problems currently experienced in practice but they will probably change with time, technology development and wider usage of the technology.

9 Dealing with the problems in practical situations

This section will address some of the ways, techniques and technologies that are currently being used and are planned to be used in the near future to fend against threats mentioned in the previous section unauthorized data gathering, denial of service attack, accessing and changing data on the tag and damaging and/or removal of the tag. Unauthorized data gathering can be successfully countered with few different approaches. Most common of them being: Cryptography throughout your system, on the tags, readers, their mutual communication and other opened systems that attacker might use;

Tag shielding or blocking – introducing radio impenetrable material between the tags and the potential attacker or electronically jamming any unwanted radio communication or eavesdropping attempt;

Minimal exposure of the tags in uncontrolled environments – faster shipment and dealing with the goods outside direct influence of the company – distribution, customs, etc.;

Using techniques like Limited successive tag queries – this technique limits the number of read attempts that can be made in a succession thus making it hard for attacker to break the tags encryption or another kind of protection and it also exposes the attacker for longer time making him easier to spot and stop.

Control systems – having people or a surveillance systems installed around and inside your premises and along your supply chain greatly increases level of security and significantly hampers any attack attempts Denial of service attack presents a real danger so measures against it have to be thoroughly considered. First way of performing denial by interrupting reader-to-tag communication requires significant technical knowledge and cumbersome equipment which allows for easier detection of the intruder who, due to the low range from which attack can be performed, has to be in, or near surveillance monitoring area. Added to that this attack is also performed for a prolonged time span and that makes attacker even more vulnerable to detection. This means that good surveillance, constant control of the facilities and your goods and preparedness to react if suspicion of attack occurs makes you highly resistant to this kind of threat. It is very important to point out that this attack denies you service only while the equipment is active so when intruder is detected and disabled your systems should be up and running. On the contrary when you have second type of denial attack and your IT systems are damaged, you have a system crash or any other problem with your systems that will not just go away if the attack it self is stopped. These attacks are much harder to detect and prevent than the previous two, but because they don't differ much from what IT experts are facing in other systems and industries daily, for many years now, there are many different ways to secure your investment. Because it is an old problem not so much RFID specific (it only magnifies in RFID systems) here we will just refer to existing IT practices and techniques. Unwanted tag data change is probably one of the easiest problems to solve and on top of that, probably one of the cheapest of all named. Even though it received a lot of publicity because it is easily imagined and because it is immediately recognized as illegal it remains less of a worry than some other mischief. In case of end of supply chain's POS locations where RFID is item based and cheap tags are the rule, than write once read many tags are good way of avoiding tag rewriting. Other cases that include large packaged or expensive goods, reusable packaging (containers, pallets, boxes, drums)and products that require rewritable tags, problems like this can be handled uncouple of different ways.

'Adequate encryption' can prevent of significantly hamper any data changing attempts; Physical protection of the tags form unwanted queries – if using
some sort of tag shielding tags are not accessible thus not rewritable; Limited successive tag queries as mentioned previously can provide some valuable time here to allow for intruder to be discovered; In case of warehouses, POS or distribution centers good surveillance is also of great help because for data change to occur intruder must get fairly close to the tag mainly because of its short range. Constant products monitoring – when you have your products constantly monitored with strategically placed readers, every change that happens with tag data or for that matter with any product can be noted by your systems and you can be notified that there might be a problem. Damaging and/or removing the tag as problem can be avoided or if not avoided then at least timely dealt with in several ways:

Protecting the tag from the damage in the first place by:
Incorporating tag into the product;
Installing tamper proof and pressure sensitive tags that are in use to certain extent in organizations already;
Avoiding unnecessary exposure of the tags to the elements.

Constant monitoring as mentioned earlier presents great solution for problem detection which is also true in this case because this kind of system should be able to detect that it stopped reading certain tag which has been damaged and report it instantly. There should be system in place or at least procedure that will effectively and rapidly substitute damaged tag or the whole product in order to avoid any further damage. For all these problems it is good to have some sort of backup systems, plans of action and intervention teams to tackle the problems when they do occur.

10 Conclusions and Recommendations

Security is of great concern to many in business world today no matter which industry or which nationality they belong to. As it was presented with this thesis, securities in RFID enabled organizations process are not any less important than elsewhere and is probably even of greater importance. Existence of the security problems and some possible solution to them were found and confirmed from literature consulting current research, from interviewed experts and experiences in the field.

10.1 Conclusions

It is astonishing how a modest device like an RFID tag, essentially just a wireless license plate, can give rise to the complex mélange of security and privacy problems that we explore here. RFID privacy and security are stimulating research areas that involve rich interplay among many disciplines, like signal processing, hardware design, supply-chain logistics, privacy rights, and cryptography. There remain connections to be explored between the work surveyed here and other areas of study. We conclude by highlighting a few of these.

It is unmistakably clear when you go through this research that problems with RFID security are many and that there is nomadic wand that can just wave them away. In order to make their recognition and the ways to deal with them more acceptable and easier for the interested participants this research had two questions to answer. As an answer to the question of this research 'What are potential security problems of RFID and suggested solutions?' the following was created combining and comparing literature findings and practical experience:

We can conclude that there are four major problem groups addressed in literature and experienced in practice and they are as follows:

- **Problems related to data stored on the tag;**
  Unauthorized reading the tag;
  Unauthorized changing the data on the tag;
  Eavesdropping on the communication between tags and readers.
- **Problems related to protection of tag integrity**
  Physical damage/removal of the tag;
  Killing' of the tag.
- **Problems with securing data related to the serial number on a tag, which may be stored in a network database**
- **Problems related to denial-of-service attacks**

The problems that were identified as most common, most probable and potentially most damaging, range from sophisticated highly technical invasions of

company's security to less technical and even pure physical destruction of RFID technology. For companies to prevent and/or handle these potential problems they need to be equally creative and smart in enabling countermeasures. These protective measures also need to cover entire range from highly technical to purely physical deterrents. Answer to the main research question 'What can companies do to avoid or combat security problems of RFID' was delivered as follows:
First, companies and responsible people in those companies need to realize and except two very important facts: RFID is here to stay and RFID as a technology has potential security problems.
Second people also have to be aware that pilot projects, on which many future predictions, policies and current development is based, are inmost cases, security wise, far away from the situation where whole process is RFID enabled.
Only when first two concerns are accepted and recognized by the companies we can move to direction that is more practical and explain what technologies and techniques companies can use in their quest for security.

Prevention:

- **Technologies**

Cryptography - for tags, tag-to-reader communication, databases Tamper proof tags – for physical protection against tag damage /removal
Product incorporated tags
Limited tag quires
Read only tags – protection against re-writing
Tag shielding – prevent tags to be read in 'hostile' environments
Limited successive tag queries

- **Techniques**

Premises surveillance – video and physical (people)
Security polices and procedures – that all employees will be familiar with
Keeping goods in readers range at all times – to spot any tampering or theft
Minimizing time that goods spend outside direct control of your supply chain
Educated employees – on possible problems and prevention

Handling problems when they arise:

- **Technologies**

Backup systems – for databases and other vital computerized systems

- **Techniques**

Incident and damage control polices and protocols

- **Established response teams**

Educated employees – on possible problems and their handling thinking in terms of 'we don't have competition' or 'everybody likes us so nobody will spy or steal from us' is naive and highly risky in RFID enabled organizations. The main reason being that material gains or material damages aren't the only motivators that you could expect people to be driven by. In today's world of high technology and incising number of tech wizards, it only takes one angry or dissatisfied

customer with the right expertise to make you' suffer'. In this case scenario you may even have some warning of things to come (an angry customer) but you would probably get no such warning in a case where some overindulged, under stimulated, 'cyber' kid wants to test his skills and hacks your system just for fun and in a process causes you to lose fortunes.
Thinking needs to be changed as the most important and crucial part of the process of making the RFID enabled organizations secure. Another contributing factor to the increased security vulnerability is level of automation, as it increases so does the number and significance of potential security problems.

Not all of the problems mentioned in this research are RFID specific and some of them are not even directly related to RFID technology, but they're also a part of this research because they will be magnified by RFID implementation or just because of the fact that they will not be eliminated with introduction of RFID and thus will still need to be consider as threats.
The fact that you cannot think of any bad case scenario right now doesn't mean that some other ill intended person will not do it or is not doing it right now.
There is no perfect solution that will eliminate every security risk there's and problems named by this research paper are neither all there are nor applicable to all situations.
RFID has problems, off course nothing's perfect, but this technology can result in great benefits and widely desirable cost savings and business growth, so the time is right, you should jump on the 'RFID train' while it is stills low moving, because when it gets going you will be left standing on the sidelines with a big question in your mind, why was I late.

Problems named earlier present a real danger to the companies as we have shown through this thesis, that's why we also gave some ideas on what are the options to combat those problems. So far, we did it only generally and that is really of no use if you don't know where and when to apply certain technique, technology or policy, that's why in following part of this chapter more detailed guidance and recommendation is given on the subject at hand.

10.2 Recommendations

In the following paragraphs further recommendations will be laid out in relation to the main research question and more practical answers will be given.
Proper risk analysis should be performed to determine how high particular risk is, what is the probability for it to happen and what are its effects. This should be done for each particular business, because you don't want to end up implementing RFID based on great promises for cost or other savings and than find yourself increasing your costs and multiplying problems.

Standard Risk management procedures are highly recommended for developing and implementing a secure RFID implementation. These procedures normally include

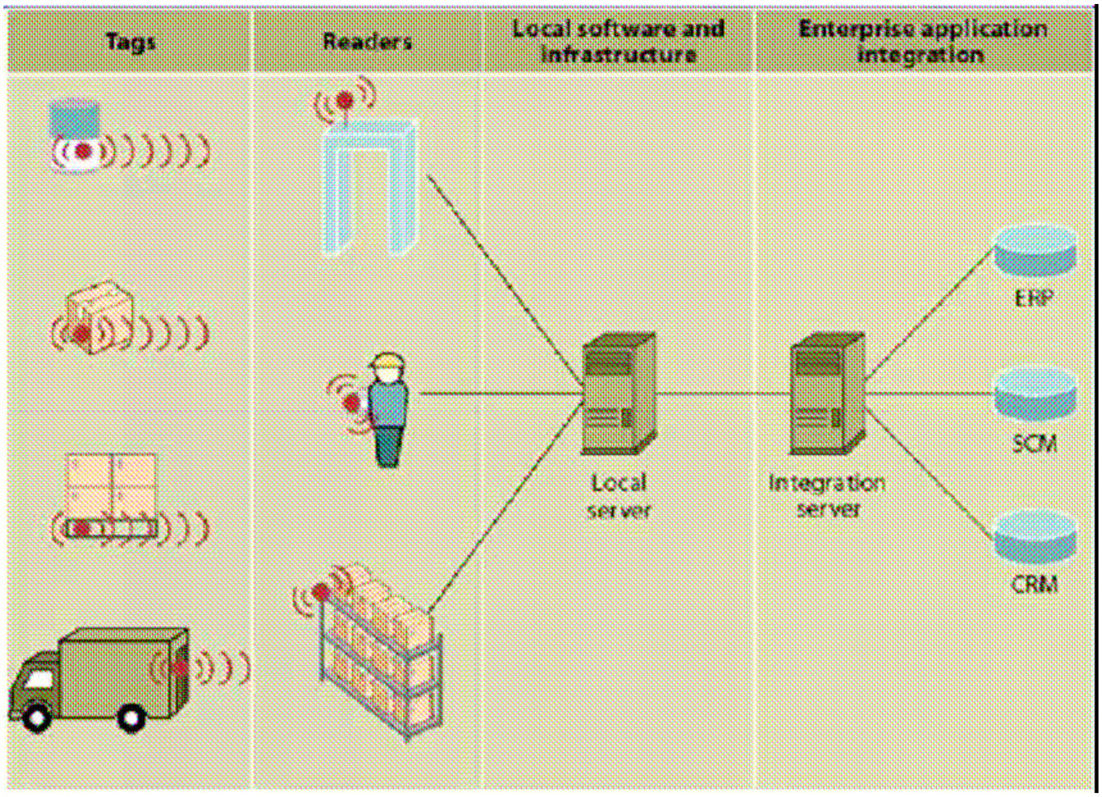
Risk identification - (in this thesis addressed as problem)
Assessment - Once risks have been identified, they must then be assessed as to their potential severity of loss and to the probability of occurrence. (That was done to some extent with more general approach in this research. Any future cases would need to be assessed individually).
Possible actions available - (relates to prevention and problem handling findings of this research)
Plan creation - Decide on the combination of methods to be used for each risk.
Implementation - Follow all of the planned methods for mitigating the effect of the risks.
Review and evaluation of the plan – These last three procedures weren't included in this research because they are very situation and company dependent.

As you could see from this paper security is not only dependent on threats in the RFID systems, the whole system is important in security perspective. That's why in parts of organization process like retail, cheep tags offer no protection by them self but when integrated with other security measures they can produce admirable results.
Even though with the implementation of every new technologies in business world people get substituted and treated as cost cuts, human factor should remain in RFID enabled organizations for control purposes because no amount of computing machinery can substitute the greatest computer of thermal, the human brain. It should be stressed that this is not all that RFID brings and it is hardly possible that 100% protection will ever be available but it is always been the game of risk management. Detailed explanation of each particular problem and suggestions to solve them has already been given throughout this research paper .

Recommendations given to particular problems listed above were selected on following criteria:
Their financially viability – in most cases you can buy almost perfect protection but the costs are to high and unacceptable;
Their level of protection to cost ratio – some solutions got priority over others because they were delivering much higher security levels per invested money units;
Ease of use and application – systems that are very secure but are difficult to implement and/or use are left behind more user-friendly solutions. These criteria were recognized from relevant literature and practical situations as being most relevant and most used. All these criteria have financial (cost) perspective as their basis because most implementers, as we mentioned in both literature review and practical part of this thesis have costs as their priority at this stage of RFID development and implementation

Company experts need to determine for them self in which category from the above they belong and if necessary apply suggested problem solutions. Some security risks are just too expensive to physically counter from so purchasing an insurance policy might be a good idea. Even if you have all these problems solved bare in mind that this is technology that is constantly and rapidly enveloping and that today's best practices can be tomorrow's losers. There is no time to stop and relax you have to keep vigil for new potential problems and developments to prevent and future misfortunes.

In implementing, operating and future development of RFID, I wish as all great success.


Tags
Readers
Local software and infrastructure
Enterprise application integration
Local server
Integration server
ERP
SCM
CRM

Source: Confino, J. & Elmore, A., 2004 RFID Fundamentals

Dictionary:

Active Tag The tag has a battery that is used as an energy source for the microchip.
Centralized data storage In the centralized approach a database holds all the data which a system needs to be able to generate usable information.
COM **C**omponent **O**bject **M**odel, a Microsoft specification for the development of object-oriented programs that enables interaction between the programs. Any COM-object can communicate with any other COM-object even though they were created for different purposes by different suppliers.
COP **C**ostumer **O**rder **P**oint - is the point in the production flow where the costumer makes his/her order.
DCOM **D**istributed **C**omponent **O**bject **M**odel, are the same as COM but with the difference that they are distributed i.e. they can be saved on different servers.
Decentralized data storage n the decentralized concept the information is moved down from the database one or many levels and is saved locally.
EAN **E**uropean **A**rticle **N**umbering - A European standard for article numbering.
EDI **E**lectronic **D**ata **I**nterchange- is a standard format for exchanging business data.
EPC **E**lectronic **P**roduct **C**ode - UCC and EAN have merged and created EPC global Inc which is a company responsible for several standards within the RFID technique.
ERP **E**nterprise **R**esource **P**lanning system – A data system which supports the planning of the resources in a company. It contains different integrated modules which support different areas of the company e.g. personnel, customers and logistics.
Escort memory A passive R/W tag with a memory of 112 b, used in the Paint shop.
Frequency For a varying current, frequency is the number of complete cycles per seconds. Measured in hertz (Hz).
Hertz The standard unit of frequency. 1 Hz is one finished cycle per second.
IMS **I**nformation **M**anagement **S**ystem. It is composed of two different systems, a database manager and a transaction manager. It handles transactions between different systems and databases.

Interface Consists of for example, graphical display formats, operating systems, key boards. Equipment which enables communication between human and machine.
ISO **I**nternational **O**rganization for **S**tandardization (ISO) – A leading worldwide organization that set standards. All standards ratified by the ISO are based on open technology.
JIT **J**ust **I**n **T**ime – A logistic method used for delivery of goods to for example a factory. The philosophy is to reach stockless production.
Killing the tag – process of using software commands to disable the tag and prevent its further usage, can be temporarily or permanently,

LAN **L**ocal **A**rea **N**etwork – a network used to connect computers and other devices in a local area like an office. It becomes a network within one are e.g. a company.

MTBF Mean **T**ime **B**etween **F**ailures. The time between breakdowns for a system or a device.
OLE Object **L**inking and **E**mbedding, the COM-based foundation of data access in the Microsoft world.
OLE COM Object **L**inking and **E**mbedding **C**omponent **O**bject **M**odel. See separate descriptions.
OPC Object Linking and Embedding (OLE) for **P**rocess **C**ontrol - This is an open standard for integrating industry systems.
Operators Some of the employees who work on "the shop floor" in the plant.
Oracle A relational database which supports SQL.
Paint shop One of the investigated areas at VTU. This is where the cabs are painted.
Passive tag The passive tag has no battery and takes its entire power from the reader.

PLC Programmable **L**ogic **C**ontroller – A control system that is often used in the industry to controls signals and machines.
POS – Point Of Sale
RFID Radio-Frequency Identification,
R/W Read and **W**rite – One type of memory on the tag. The company could change the information on the tag as many times they want. The tag could also be red as many times the company wants.
Rack A rack is used as a transport frame for the details in the Paint shop.
Reader A data capture device that communicates with tags, application and computer networks. A part of the RFID system.
RO Read **O**nly – One type of memory on the tag. The tag has a specific ID-number that the manufactory company has saved on the tag. The information on the tag can not be changed. The tag could be read as many times as the company wants.
SCADA Supervisory **C**ontrol and **D**ata **A**cquisition- A system that is used to present process-data from control systems. One example of a SCADA system is SIMATIC WinCC.
Semi active/passive tag The semi active/passive tag has a battery which powers the microchip. This makes the answers faster to the reader.
SIMATIC SIMATIC is an automation system manufactured by Siemens and has different functions like WinCC.
SQL Structure **Q**uery **L**anguage – A type of programming language.
Supply Chain The supply chain is the different flows that exit between actors in a products life. The actors in a chain could for example be supplier-producer-distribution-dealer-costumer.

Tag A device which consists of a microchip, antenna and sometimes a battery (see active, passive and semi tags). On the tag, data is saved which is read by a reader.
TCP/IP Transmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol. A protocol is a communication language and TCP/IP is dedicated to the internet. It is also used in private networks.
UCC Uniform **C**ode **C**ouncil Inc. - An organisation which covers global e-business communications standards, numbering schemes and barcode standards.

UHF **U**ltra **H**igh **F**requency - 860-960 MHz. A frequency band that is used in communication between the reader and the tag in the RFID system.
VCN **V**olvo **C**orporate **N**etwork is the network which all companies within Volvo Corporation use.

W3C **W**orld **W**ide **W**eb **C**onsortium is an industry consortium which creates standards for the Internet.

WinCC **Win**dows **C**ontrol **C**entre - WinCC sends and collects data to
and from control systems and databases.

WORM **W**rite **O**nce **R**ead **M**any - One type of memory on the tag. The tag has a specific ID-number that the company itself can write once. The tag could be read as many times as the company wants.

REFERENCES

1 http://www.rfidjournal.com.

2 http://www.alientechnology.com.

3 http://www.boycottbenetton.com.

4 http://www.ecrypt.eu.org/stream/.

11 http://www.rsasecurity.com/rsalabs/node.asp?id=2115

5 http://www.ti.com/rfid/docs/manuals/pdfSpecs/epc inlay.pdf.

12 Gibbs, T., 2004. RFID: The Next New Thing. Intel Corporation. Available form: http://www.ascet.com/document.asp?d_id=2539.

13 Sule, S., Avhad, S. 2003. Is RFID a Disruptive Technology? Patni Computer Systems Ltd.

14 Berthon, A. & Guillory, M., 2000. Security in RFID. Texas Instruments and Intermec Technologies. Available from: http://stud.ita.hsr.ch/ss03/ss0304/

15 Claburn, T. & Hulme G., 2004. RFID's Security Challenge. Available from:http://www.informationweek.com

16 Hesseldahl, Arik, 2004. A Hacker's Guide To RFID. Available from: http://www.forbes.com/commerce/2004/07/29/cx_ah_0729rfid.html

17 Hulme, G., & Claburn, T., 2004. RFID's Security Challenge. Available from: http://www.informationweek.com/story/showArticle.jhtml?articleID=52601030&tid=13690

18 Rothfeder, J., 2004. What's Wrong With RFID? Available from: http://www.eweek.com/article2/0,1759,1634129,00.asp

19 S. Garfinkel and B. Rosenberg, editors. RFID Applications, Security,and Privacy. Addison-Wesley, 2005.

20 Eric Lundquist . The Real RFID Security Issue available from http://www.eweek.com/article2/0,1895,1941421,00.asp

21 Thomas Claburn George V. Hulme . RFID's Security Challenge available from http://www.informationweek.com/story/showArticle.jhtml?articleID=52601030&tid=13690