A Feasibility study of new RFID Applications

By

Trond Henning Johansen
Ørnulf Storm

Masters Thesis in
Information and Communication Technology

Agder University College

Grimstad, June 2004

Abstract

The introduction of Radio Frequency Identification represented quite a revolution to the various areas of industry and business, focusing on the process of marking items for automatic identification. RFID offers similar functionality as the well established barcode, but with major additional advantages. These are in short read/write capability, memory, and operation independent of free line of sight between reader and tag. Enhanced production techniques also seems to contribute to lower production cost and thus cost per unit boosting the research on new and promising RFID applications.

Other factors contributing to the adoption of RFID technology is the tendency of multinational companies as Hewlet Packard and Microsoft to join the global initiative of RFID standardisation. EPCglobal was launched by an European, American and Asian initiative lead by respectively EAN International and UCC. Another matter is the fact that widespread use of ISM frequecies simplifies the role of national legislation Finally the issues of ethics and privacy are to be adressed as this is about to be a major problem regarding RFID technology and thus a potential hurdle for further progress and comercial success on a global basis.

In this report we focus on recent research projects, driven by features as integrated sensors, memory, and processing capacity. Based on this we aim to call attention to a limited number of promising applications which will be evaluated against a number of criterias in a framework developed especially for this master thesis, adressing matters such as frequency and range, active or passive transponders, memory requirements, dependency of ongoing or future standardisation, radio regulation and privacy contraints. We will also discuss external factors such as the influence of tag price and numbers of items to be tagged in the applications. By discussing each of the chosen applications in relation to the selected criterias we found which applications that appeared to be of particular interest comercially and thus recommendable for actual implementation. We have made the conclusion that several of the new promising RFID applications are ready to be launched and would have potential good prospects for future use.

One major obstacle for sucessful implementation appears to be the privacy issue. With this issue under control, launching a Supply Chain Managagement system as a global reaplacement for the bar code system using tags stardardised by EPCglobal would have very good prospects for being sucessful within a few years. Immediate implementation would only be possible in small scale, but in late 2005 larger implementations seems very likely, if standardisation of ECPglobal has settled. Also asset tracking of important or valuable items as well as tracking of persons could have good chances of looking at sucessful implementations in the near future as long as the privacy issues are taken taken into careful consideration.

Due to the ongoing work on standardisation it seems like at small pilot would be appropriate in order to reduce potential loss due to changing standards. This would provide valuable experience in handeling the technology while awaiting the standardisation, etichs and privacy issues to settle. Furthermore it seems that pilots featuring passive technology would contribute to lowering the risk even further as the marking of numerous items by active technology could imply rather high costs.

Preface

This thesis concludes the Master study within the field of Information- and Communication technology at the Agder University College, faculty of engeneering and science sited at Grimstad, Norway. Our curiosity for the RFID technology was aroused in the late autum of 2003. Related to another subject taught at HiA we got involved in a project linking patients and bloodsamples by providing both with RFID tags for unique identification. By doing this we expected to reduce the possibility of mismatching pairs of patients and coresponding bloodsamples. By the end of the project we realised the tremendous scope of possibilities lying within the technology of RFID. Among a number of master thesis' offered by Agder University College and others was the opportunity we had been waiting for. "What is RFID and what can it be used for?" was the original Norwegian title chosen for this thesis given by Teleca., an enterprise well known for delivering GPRS solutions to Ericcson still on search for new interesting prospects featuring wireless technology. By introducing the reader to, both present RFID technology, as well as a glimpse of the future, we hope this perspective is about to become slightly clearer.

Finally we would like to express our gratitude to Teleca, represented by BScwHon Espen Heggelund, BSc Ole Jonny Gangsøy, and BScwHon Jøran Bøch, for excellent guidence and advice in the process of producing this document. We would also like to thank assistant professor Arild Haglund at Agder University College.

Trond Henning Johansen

Ørnulf Storm

Grimstad, Norway June 2004

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Thesis introduction

Teleca is a multinational consulting company operating within the field of wireless solutions specializing on delivering GPRS technology to Ericsson. In their search for alternative business areas, RFID has come up as one alternative technology worth looking closer into. Due to technological development and maturing, new and promising enterprise solutions are emerging and many are expected to have considerable business potential. In this thesis we put focus on technology as well as other factors of importance that is expected to have influence on a new application prospects of beeing successful. The challenge of exploring the new potential of this technology has been given as a master thesis for the students as a part of the cooperation programme with Agder University College in Grimstad

1.2 Work description

The title of this thesis is “A Feasibility Study of new RFID Applications”.
Radio Frequency Identification (RFID) applications have existed for decades, but the variety and widespread of the technology has been limited to a rather small number of applications. During recent years, research and new production techniques have made RFID equipment manufacturing more cost-effective, making RFID applicable to a whole new range of applications. It is mainly in the USA and parts of ASIA that the applications have started to be used more widely other than just in small, but well known niche markets, as tolling, access control and electronic article surveillance.

In order to provide advice on what applications that could have good prospects of being successful, an evaluation of recent research and development on new applications would be appropriate. Furthermore this study will be limited to enterprise solutions only.
To be able to better understand how RFID can be used commercially, a study of the RFID technology and its characteristics is required. This knowledge will provide a foundation for understanding the limitations and possibilities of the technology when studying new potential applications.

Another important factor to consider is standardisation. The presence of standards will hugely influence on new development of applications because standards ensures interoperability across borders and between different manufacturers. This factor is likely to have great impact on the market adoption for any new RFID application. The existence of National Radio Licensing Regulations will also have an impact on the adoption of new RFID applications and must be taken into consideration.

With emerging new RFID applications, and its possible spread into new fields of utilisation, some issues of great importance appear. Crucial issues are privacy, ethics and security and these could all have an impact on the use and distribution of new applications. These must therefore be taken into consideration and handled with outmost care.

Teleca Wireless Solutions (TWS) [1] has already a very good knowledge of wireless communications and General Packet Radio Services (GPRS) in particular. Therefore it is of interest to TWS to gain knowledge about potential new business areas especially within the field of wireless technology.

1.3 Literature review

This section explains where we have obtained relevant information for this thesis. The information used has been taken from variours sorces. One main source for the theory is the "The RFID Handbook" by Claus Finkenzeller [2]. Information on Standardisation is taken from various standadisation organisations such as, ITU, [3] ISO [4], CEPT [5], ETSI [6], EPCglobal [7]. Several of the case studies of applications is taken from RFID Journal [8] which is a respected resource for reliable information on RFID technology. Information of new products and possible future applications are collected from various RFID product manufacturers, RFID Journal and Research Institutes like Massachusets Institute of Technology (MIT) [9]. Reported research projects are also taken from some of the leading consultant companies.

1.4 Report structure

- The second part of this report is ment to provide the basic theory of RFID technology. This will establish a foundation for understanding the RFID concept.
- The third part will give an overview of current standards, organisations, and ongoing work on standardisation.
- The fourth part will provide information on radio regulation issues
- The fifth part will discuss ethics, privacy and security issues related to RFID.
- The sixth part will give the reader an overview of existing RFID applications and thereby introduce the reader to the current usage.
- The seventh part will give examples of new resarch leading to new applications. This part will provide the latest resarch activities for RFID and will be the basis for discussion of what could be promising future applications.
- The eight part defines a framwork which is used to conduct an evalutation of new RFID applications. The development of the framwork is also based on the set of properties and selection criteria expected to be of vital importance for the new RFID applications.
- In the ninth chapter we are using the framwork to evaluate 5 different new RFID applications.
- The tenth and last part gives a conclusion on what applications that could have good prospects to become successful. The conclusion is based on the results documented in the previous chapters of this report, and give our conclusion on the possible prospects for 5 new RFID applications.

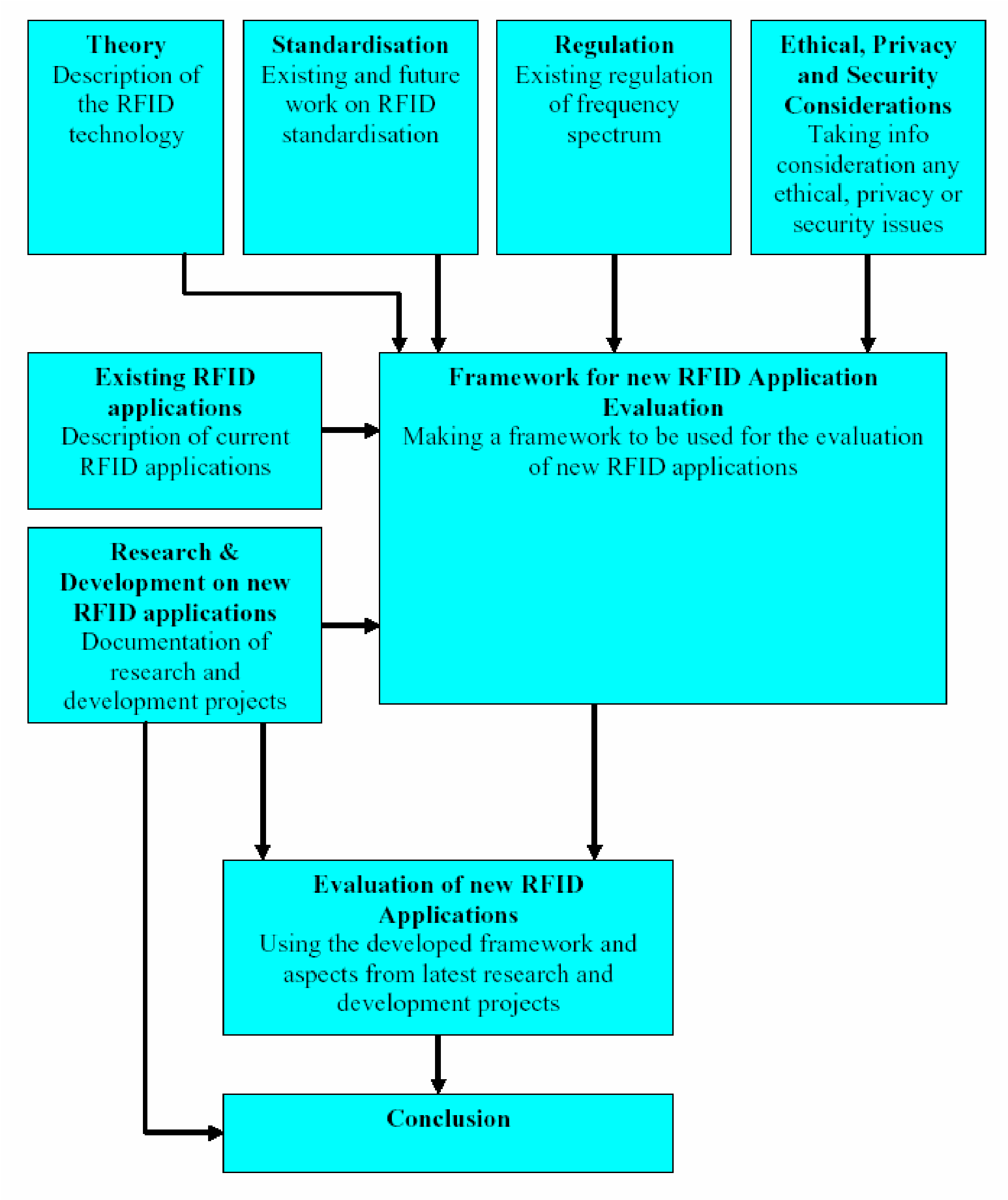

Figure 1 - Graphical description of the report structure

2. Radio Frequency IDentification

2.1 A brief introduction to RFID technology

Radio Frequency Identification has in principle been around for some time with the RADAR being one of its early ancestors by its introduction during WWII. This concept allowed pilots to identify an incoming airplane as friend or foe. RFID technology as such has a history back to the late 60's and early adoptors were identification of live stock and tracking of rail cars in the USA. In the mean time we have learned to enjoy the benefits of wireless communication by mobile phones and through broadcasting of television- and radio transmission.By emitting radio frequency energy, the RFID reader interrogates its surroundings for the precence of a RFID tag marking an object of interest. When exposed to the radiated power, the tag responds by transmitting selected information back to the reader using the received energy as its source of power. In its simplest form the tag returns a pre-programmed serial number or even a singel bit in contrast to more sophisticated cases adding capabilities of on-board memory and sensors as well as data-processing capabilities by integrated microprocessors. This is due to intensive research within the field of VLSI production techniques and low power circuits making the production of miniature RFID tags with high efficient on board batteries possible. Another trend of great importance is the ability to equip tags with different kinds of sensors capable of measuring quantities as temperature and pressure from the surroundings. Finally there is a rapid increase in available on bord processing capacity leading the way to a brand new range of promising applications to be launched.

2.2 Comparison of RFID to other related technologies

Over the years many techniques for automatic identification (Auto-ID) have been launched with various success both tecnologically and comercially. In addition to RFID there are related concepts as Optical Character Recognition (OCR), Smart Cards and Biometrics in addition to the well established barcode. The latter being frequently compared to RFID, still barcodes are cheaper to produce and therefore still dominates the marked. Advantages of RFID compared to bar-codes are numerous. Most obviously is the advantage of non contact and non line of sight offering a tremendous gain compared to bar codes. Tags can be easily read through a number of substances such as paint, clothing, light walls, rain, snow and fog. All cases where barcodes would prove useless. The most important advantages in favour of RFID are as follows:

- Not influenced by dirt and moist allowing tags to be embedded into a number of materials and placed in hostile environments.
- Not influenced by optical covering allowing the tag to be read without line of sight.
- To a certain degree not influenced by position or direction.
- Durable as degradation, temperature and wear is not a major problem.
- Operation costs are next to none.

- Unauthorized copying and modification is impossible.
- Very fast reading speed in the higher frequency ranges.
- Can be read from and written to thousands of times.

Moments in favour of the barcode would still be:

- The cost of the RFID technology in general and the tags in particular is notably higher compared to barcodes. However the gap is closing in.
- Lack of global standardisation on RFID.

Table 1 - Comparison of RFID and barcode

System	RFID	Barcode
Transmission	Electromagnetic	Optical
Datavolume	128 – 8KB	1 – 100 Bytes
Susceptibility to environmental changes	Considerable	Little
Read / Write (modification)	Both	Read only
Position of reader vs carrier	Line of sight not required	Visual contact
Reading distance	10 – 20m with acive tags	A few meters
Security	Hardly	High
Anticollision	Yes several tags can be read simultanously	No

2.3 The basic concept – Reader and tag

In general a RFID system consist of four fundamental parts:

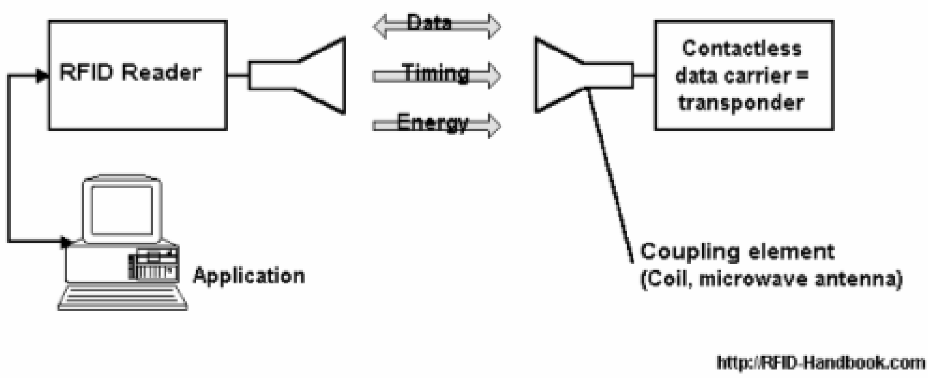

Figure 2 - RFID basic concept [2]

RFID Antenna
The reader and tag antennas are emitting and receiving the signals allowing communication to take place.By using its antenna the reader is capable of either emitting radio signals to or receiving signals from the tag. Thus the antennas enables radio communication between the units allowing data and control information to be exchanged. The shape and size of the antenna is important due to the specific use of the system. Higher frequencies in the microwave band allows higher rates of data to be transfered on the expence of communication taking place only at the line of free sight thus being vulnerable of obstacles along the transmission path. On the other hand lower frequencies are more flexible as far as obstacles are concerned at the expence of lower data rates and larger antenna size. Antennas come in a number of shapes and designs operating on several frequency bands depending on the ranges and characteristics concerned and due to the application in question. The antenna is made of wound copper wire for the lower frequencies and is just a miniteurized strip of copper for the micrwave frequencies. Modern production techniques have resulted in better antennas resulting in smaller tags that can easily be integrated in a number of materials.

RFID Reader
A reader or transceiver is the interrogating part of the system. The RFID reader is emitting radio frequency energy to its surroundings by the built in antenna. By making use of a number of predefined frequencies operating with a certain range of transmission, the tag is adressed. Depending on the frequency of use , the level of penetration will vary from total penetration of obstacles at the lower frequencies to transmission limited to free line of sight only for the microwave frequencies. When receiving an incoming signal the reader might have to separate one tag from another introducing an anti collision mechanism. Ref cars passing through a toll plaza. Other tasks might be error correction and parity checking as well as security mechanisms like encryption (confidensiality and integrity) and authentication. The reader is interacting with the connected computerhost or network by receiving commands and relaying the information collected or “harvested” from the tags.

Figure 3 - RFID reader with CF interface

RFID Tag
A tag, token or transponder (transmitter and responder)beeing an integrated circuit with memory and an antenna of it’s own allowing information to be read from or/and written to by the reader. This unit represents the addressed part of the system receiving the reader energy at its distinct resonance frequency allowing local processing and retrieval of stored information to take place due to the request. Next, parts of the energy will be returned to the reader containing the information demanded by the reader.

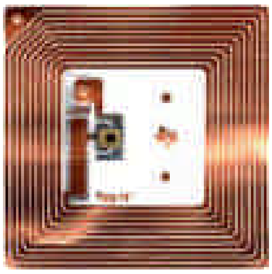

Figure 4 - passive RFID tag

Computer network or RFID application platform

A final component of a RFID system will be the associated computer network by which the reader is connected allowing the collected information to be distributed to its end users. Also the actual frequency in question is sometimes included in the system components of an RFID systems.

2.4 Active and passive tags

Tags in a RFID system can segregated into two major categories beeing **active** and **passive** tags.

Figure 5 - Example of active RFID tags

Acitve tags

Active tags are deriving their power from an on-board battery capable of supplying the circuitry with power as well as enabling a longer range of broadcast to the corresponding reader. Active tags are usually read/write devices. Furthermore active tags reduce the requirements for reader power allowing the transmission to take place over longer distances. However their lifetime is limited and they are also more expensive than passive tags. Modern technology is resulting in large scale integration and power saving circuitry allowing ten years or more of operation limited only by external temperature, duty cycles and usage. The price is bigger sizes and greater costs. Longer ranges, better immunity to noise and higher transmission rates are among the obvious benefits. The battery will have to be replaced regularely for reusable tags or used tags can be wasted as the case would be for disposable tags containing not replaceable batteries.

Figure 6 - Example of passive RFID tags

Passive tags

In contrast to active tags passive tags draw energy from the interrogating reader by current beeing inducedI in the transponder antenna. Active tags are preferred for tracking objects over longer ranges, but this is reflected in higher costs pr unit. Passive tags are lighter, smaller and cheaper compared to active tags. Their reading range is shorter and depend upon a reader with higher power. These tags are also more exposed to electromagnetic noise but their lifetime is almost indefinate.For passive tags two concepts yelds:

- Tags transmitting by reflected power only – True passive tags
- Passive tags with an onboard battery where the extra power is entirely used for enhanced data processing or to power local memory. Transmission is still depending on the power received from the reader.

To summarize:

Table 2 - Comparison of active and passive tags [10]

Characteristics	Active tags	Passive tags
Power source	Battery	Inductive coupling
Memory	Up to 288 kb	Up to 288 kb
Read range	Up to 500 m	Up to 15 – 30 m
Class	0 – read only 3 – Write once, read many 4 – Multi read / write	--------------------
Frequency	Low – 125 – 143 KHz High – 13,56 MHz UH - 868 – 930 MHz MW – 2,4 GHz	303, 433 MHz
Data transfer rate	Variable	Variable

2.5 Frequencies of use

Characteristics of the most applied frequencies will be described in the following section. The basic rules of RF transmission still applies, despite the relative short distances in question. This implies that signals of lower frequencies will posess better qualities in omitting obstacles along the transmission path compared to transmission using a higher frequency. On the other side higher frequency allows a higher rate of data to be transferred which could be cruical in applications depending on reading the datacarrying tags in a very limited amount of time, as the case would be in applications handling automatic car tolling. RFID transmission is a subject to the same laws of physics as regular radio frequency signals hence there are phenomenons like reflection, absorbtion and cancellation. There are several frequency bands in use, but a rough overview of frequencies and characteristics is documented in the table below from “RFID -A week long survey of the technology and its potential” [11].

Table 3 - RFID frequencies and characteristics [11]

Frequency	Characteristics	Example applications
Lower band 100 – 500 KHz	Short reading range Inexpensive tags and lower costs in general Low reading speed Inductive coupling None dependent of line of sight	Access control Inventory control Animal tagging
High band 10 – 15 MHz 850 – 950 MHz	Read range between short and medium Reasonably Not expensive tags Inductive coupling Medium reading speed	Access control Smart Cards
Ultra High 2.4 – 5.8 GHz	Long reading range High reading speed Line of sight only Expensive (active tags) Backscatter coupling	Automatic tolling systems Car, train or container (vehicle) identification/ Monitoring

In either case the tag is exposed to an interrogating field emitted by the reader. Being parts of the same system the reader frequency will trigger the resonance circuitry of the tag to respond by returning the desired information or simply signalling its presence. A passive tag is doing this by the sole use of the received energy returning what’s left of it through it’s own antenna at the appropriate frequency. In some cases an active tag is preferred allowing an “on board” power source to provide additional processing capabilities or power to transmit over longer distances, if required by the specific application. This enables transmission ranges up to several hundred meters.

Corresponding advantages are unlimited lifetime, light weight and cheap tags in favour of passive tags and added processing and memory capacities as well as longer ranges in favour of active tags. The operation of the reader and tag is identical to the system initially being used during WW2 allowing aircrafts to identify other aircrafts as friends or foes depending on the response of an interrogating signal being emitted in a special manner using special codes.

Memory
A factor of increasing importance is the amount of memory availiable on the tag. This is a result of a revolution in the VLSI production technology allowing new areas of use to be adopted. This, along with onboard processing capacity, is truly one of the major changes to the recent development within RFID technology . The amount of memory availiable on the tags will vary from a pre defined serial number only provided by the manufacturer during the production process to kilobytes of memory allowing considerable amounts of data to be stored. This memory could be read only or more likely a memory for both read and write operations. The figure below indicates the connection between tag functionality and memory capacity.

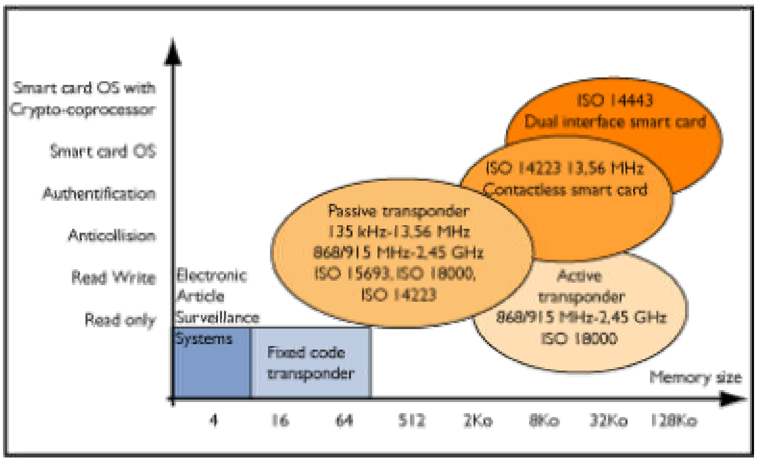

Figure 7 - Memory capacity in relation to functionality [12]

2.6 RFID Systems

Basically the operating procedures describes the interaction between transponder and reader. The two main issues are the transponders power supply and the data transfer between the transponder and the reader. A lot of the following information has been extracted from the RFID Handbook [2].

3 main operating procedures applies:

1. 1 bit systems
2. Full and half duplex systems
3. Sequential systems

2.6.1 1-bit systems

5 types of 1-bit system exists. The 1-bit transponder is used in a wide range of applications, amongst them the electronic anti-theft system called EAS, Electronic Article Surveillance. 5 different operating principle for the 1-bit transponder exists. The procedures are Radio Frequency, Microwaves, Frequency divider, Electromagnetic and Acoustomagnetic.

Radio frequency
The transponder is a LC resonant circuit. The reader is a sweep generator that sweeps $f_0 \pm 10\%$ and f_0 is the resonant frequency of the transponder. If a transponder is in the range of the reader when the frequency is the resonant frequency the voltage drops in the generator coil in the reader and this is detected. This is how the reader detects a transponder withing the range of the reader. To deactivate the transponder it is exposed with a very strong magnetic field that destroyes the transponders foil capacitor. Example frequency areas are 1.86-2.18MHz, 7.44-8.73MHz, 7.30-8.70MHz and 7.40-8.60MHz.

Microwaves
The transponder is a nonlinear capaciance diode connected to the base of a dipole which is adjusted to the carrier wave. The carrier wave can be 2.45GHz, 5.6GHz or 915MHz (outside Europe). For detecting an article with an transponder a transmitter operating on the carrier frequency is placed close to the exit of for example a warehouse. The carrier frequency is modulated with a 1kHz signal using amplitude shift keying. When the signal reaches the transponder the transponder transmits harmonic frequencies of the carrier frquency. The 2^{nd} harmonic frquency is detected by a detector which demodulates the signal. If a 1kHz signal is detected the systems sounds an alarm.This system is mainly used for textiles.

Frequency divider
The transponder is a resonant circuit with a microchip with devides the received signal and sends it back to the reader. The reader is transmitting on the resonant frequency, but listening for half the resonant frequency. This procedure also used a amplitude shift keying modulation technique to avoid noise causing false detection. The operating frequency area are mainly in 100-135.5kHz.

Electromagnetic
The transponders are soft magetic amorphous metal strips. When exposed to an strong magnetic field from the reader the transponder are generating among other frequencies also differential frequencies of the supplied signals. When the reader detect these differential frequencies it knows that a transponder are in the vicinity. The reader generates electromagetic fields in the frequency area of 10Hz to around 20kHz. These systems are the only systems suitable for products containing metal.

Acoustomagnetic
The transponder is in this case an amorphous metal strip constructed to have a specific acoustic resonant frequency. When exposed for a magnetic field from a transmitter it starts to oscillate. The oscillation of the transponder are detected at the exit door of a shop by a receiver tuned to the specific resonant frequency. Typical frequencies used are 12Hz, 70Hz, 215Hz, 3.3kHz and 5kHz.

2.6.2 Full and Half Duplex Procedures

These systems normally use an electronic microchip as the data-carrying device with a data storage capacity of a few kilobytes. For full duplex systems the data transfer between reader and tag, and between tag and reader respectively, is happening at the same time.

Inductive coupling

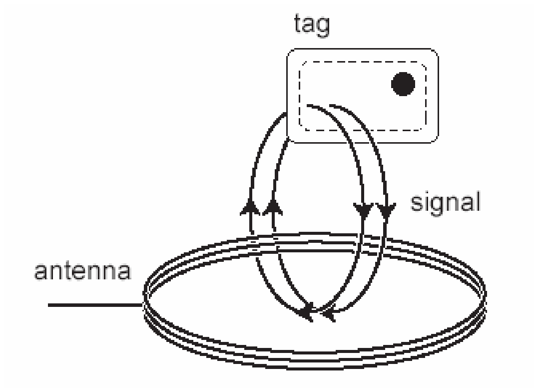

Figure 8 - Inductive coupling [11]

Elements of an inductively coupled transponder are an electronic carrying device consisting of a single microchip and an antenna in the shape of a coil.
Almost always operated passively meaning that all the required power is supplied by the reader. By providing an electromagnetic alternating field to cross the windings of the transponder antenna, current is induced enabling the local processing to take place as well as providing power for the retransmission / reply to the readers request. The frequency interval taking advantage of this effect is between 135 KHz and 13.56MHz respectively representing wavelengths of 2400m and 22.1m. These wavelengths being much longer than the distance between reader and tag means that the energy transfer is due only to the effect of the alternating magnetic field being a "near field" effect only. A voltage is thus induced in the receiving antenna coil. This voltage is rectified and next used to power local processing and memory management as well as the response to the reader. A capacitor across the antenna coil allowing a certain resonance frequency to be determined in accordance to the transmission frequency of the reader. This effect is closely related to the primary to secondary coil relationship well known from transformer theory. This relationship yields when the distance between tag and reader do not exceed 0.16λ meaning that the tag is located in the near field of the interrogating reader. A resonant transponder will draw energy from the emitting reader causing a voltage drop over the internal resistance of the reader

antenna. These voltage changes will cause the alternating field to vary thus changing the amplitude of the field at the transponder end of the system. By superimposing information on these variations a transfer of data can be established by the principle of “load modulation”. At the reader these variations are rectified or “demodulated” and reinterpreted as information. Load modulation generates exstremely weak signals which have to be filtered and processed in the interrogator.

Electromagnetic backscatter

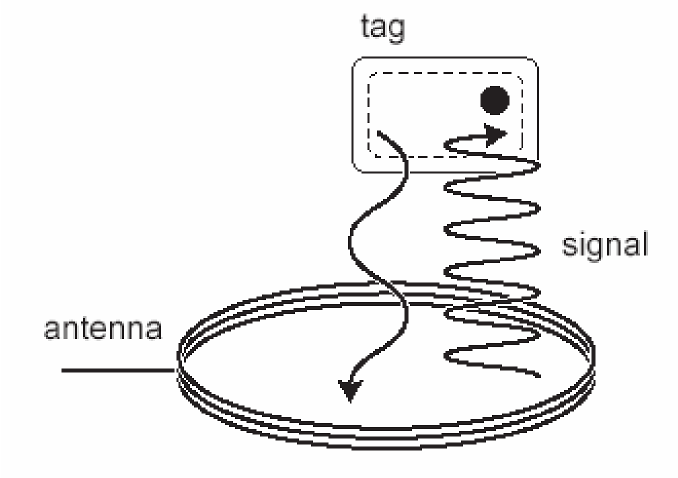

Figure 9 - Electromagnetic backscatter coupling [11]

This principle resembles the RADAR effect by the partial return of emitted energy as a result of reflection from an encountered obstacle along the signal path. This applies for obstructions being larger than half the wavelength of the emitted wave. Another factor to take into consideration is the “reflection cross section” of the object which is particularly favourable when in resonance with the signal emitted by the reader. A small proportion of the received power is received by the transponder antenna, rectified and eventually serves as power supply for the tag circuitry. Another proportion of the received power is reflected by the antenna and can be used to modulate a tag response to the reader thus the term “backscatter”. This power is radiated into free space as true RF energy from where a small fraction is intercepted by the reader antenna. The original signal emitted from the reader is stronger by powers of ten and suppressed by couplers by arrival at the reader.

These systems have a longer range than the inductive coupled systems and typically 1-15 meters. The power transfer from reader to transponder are conducted by receiving the radiated power using a traditional free space path loss calculation in the same way it is performed for microwave systems. To atchieve a better range the transponders may have a battery for power sypply in addition. Typical operating frequecies are in the UHF band utilising 868MHz in Europe (915MHz in USA) and 2.5GHz and 5.8GHz.

The data transmission from transponder to reader are performed by a method called Modulated reflection cross-section og modulated backscatter. Some of the transmittet RF power are reflected back from the transponder in the same way as when radar beam hits a plane and is reflected back.

Electrical coupling

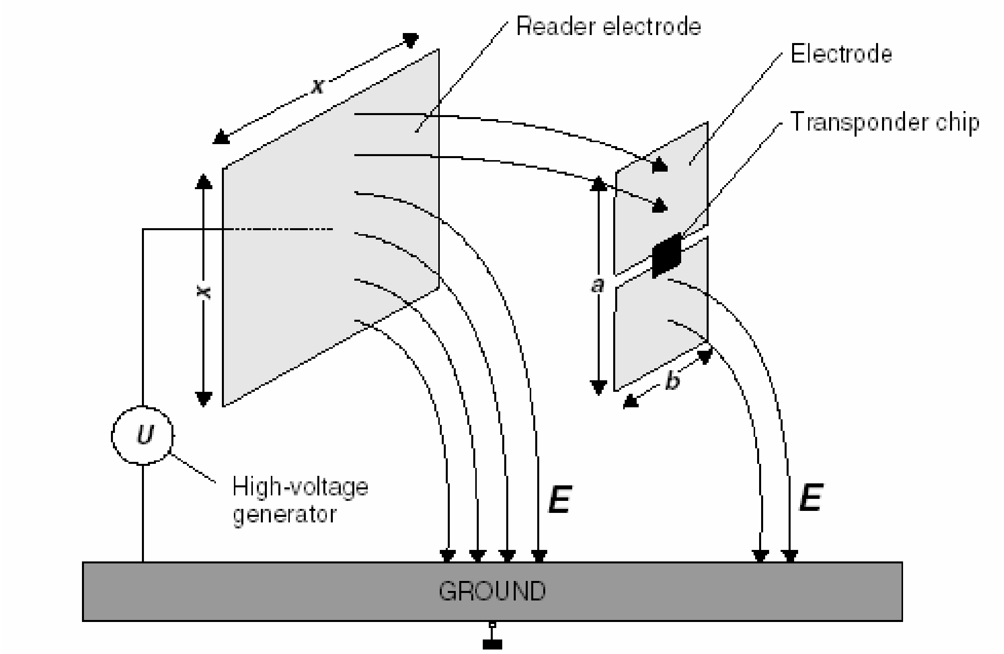

Figure 10 - Electrical coupling [11]

For this procedure the reader is generating a strong high frequecy electrical field. The reader antenna is made of an electrode made by metal foil or a metal plate. The antenna element of the transponder are also electrodes tuned to the resonant frequency of the reader. Swithing the modulator resistor in the transponder on and off an amplitude modulation of the voltage in the transponder is generated. By switching the resistor on and off in time with data it can be transmitted to the reader. This procedure is as previous described and is called load modulation. For all the procedures for full and half duplex systems described above the data transfer from reader to transponder are performed in the same way. Three basic procedures can be used. These are amplitude shif keying, ASK, frequency shif keying, FSK and phse shif keying, PSK. The most common used method is ASK modulation because of its simplicity.

2.7 Sequential Procedures

When the transmission from reader to transponder and transponder to reader are not conducted at the same time we call the procedure sequential. This is basically the same as time division multiplexing. The sequential systems using inductive coupling are normally used for frequencies below 135kHz. The readers generated magnetic field are inductively coupled to the transponders coil. The induced voltage in the coil is rectified and thereby used as power supply for the transponder. Because the power transfer is not continous the transponder uses a capasitor to store the power that has been transferred. To be able to send data form the transponder to the reader the HF signal is FSK modulated.

2.8 Anticollision Procedures

When accessing one single tag anticollision is no issue. When accessing several tags within the RFID-reader's range at the same time the issue about anticollision must be addressed. The advantage of detecting a single tag in the presence of an interrogating reader is obvious, but the true challenge remains in beeing able to detect a number of tags "simultaneously" as the case would be when a pallet of RFID marked goods is transported by truck through an electronic gate entering the stockroom of an enterprise. Beeing able to get an instant onscreen survey of the articles involved would be a large step forward for modern logistics. The feature in question is called "Anti collision" and offers a mean of avoiding all of the tags present in the reader field to transmit simultaneously. This implies mechanisms for allowing only one tag to backscatter at a given time. Obviously the operation where the tags are adressed by the reader is carried out by broadcasting the interrogating signal allowing all present tags to listen. Next the transponders will respond to the reader applying the principle of "Multi access". The challenge is thus for the reader to sort out the signal of particular interest from the rest. This is done by dividing the availiable capacity between the transponders taking part in the exchange of information and by this avoiding interference from happening. Fundamental principles also adopted in other areas of communication are the following procedures:

CDMA – Code Division Multiple Access
TDMA – Time Division Multiple Access
FDMA – Frequency Division Multiple Access
SDMA – Space Division Multiple Access

These techniques are offering multiple access on widely different terms which will not be given further attention in this thesis. Another significant problem to be adressed is the fact that the reader to tag transmission is incoherent and unpredictable taking place over a brief period of time. This requires the selection and access procedures to be both fast and powerful in order for the system to operate reliable. Associated algorithms to the multiple access mechanisms mentioned above are the Aloha procedure and the Binary search algorithm.

2.9 RFID Selection criteria

When considering new applications based on RFID technology there will have to be focus on certain requirements concerning the following aspects. This aspects will have to be carefully considered from application to application in order to get the optimal system characteristics regarding both technical performance and economy.

These criteria are:

- The speed of the datacarrying object as this might be an animal, a postal parcel beeing tracked or a car passing through a tolling station.

Within the reading zone of the interrogator the object in question will have a certain speed leaving the tag accessible for reading for a while before getting out of range. In case of a car passing a toll plaza, the availiable time for reading the tag will be shorter compared to the case of a parcel, passing a reader on a conveyor belt.

- The minimum distance between a number of tags within the readingzone.

Considering a car passing a tolling station there will have to be some slack in the car to reader distance from one passing car to another. This is due to the fact that cars can differ quite a lot in height, length and size.

- The positional accuracy of the tag

This is a term resulting from the fact that different objects will aproach the reader by different speeds thus the question is avoiding the reader to read more than one object at once causing a conflict.

2.10 The cost of RFID tags

Obviously cost is a fundamental issue when future applications of RFID technology are discussed. Implementing RFID technology for an entire enterprise might be an expensive venture. Just installing an EAS system in your retail store to prevent shoplifters from ripping one off, could differ widely in cost. In order to protect every single item one will have to equip all articles with a tag thus it becomes rather important wether there are 100 or 1 billion items to mark. Let the price pr tag vary from 50 Cents to 10 Dollars a piece and calculate the cost. No wonder the barcode is longlived and hard to compete with offering units at a few cents a piece. Still higher production volumes and polymer technology indicates that the tide will change in near future and the prices are thus constantly declining. The 5 Cent tag predicted for years has been an object of major controvercy.

“So will the promised 5-cent tag become a reality? Based on the 30 billion tags that will be needed annually and innovations that will make the industry more efficient, RFID Journal concludes that we will see 5-cent tags in 2007. But they will come initially from innovators, such as Alien and Matrics, and won't be in abundant supply. So only those companies that negotiate deals ahead of time will be able to buy them at that price in 2007."

The Case for a 5-cent Tag

It could take the consumption of 30 billion tags a year to reach the volume needed to drive tag prices below a nickel. But if just five of the retail sponsors of the Auto-ID Center ask their suppliers to tag cases, those suppliers will use roughly 10 billion tags annually.

Retailer	Annual sales	Tags needed by suppliers
Carrefour	$ 72 billion	2 billion
Metro	$ 54 billion	1 billion
Target	$ 44 billion	1 billion
Tesco	$ 42 billion	1 billion
Wal-Mart	$245 billion	5 billion
		Total: 10 billion

Source: RFID Journal

Figure 11 - Cost of tag versus order size [13]

Finally there will also be a risk related to investments in RFID technology in times where nor standards or new trends within the technology have setteled. One might buy equipment for millions just to experience that the supplier is facing bankrupcy or that the solution does not meet future needs or is not supported by standards. Most likely there will be a period of time before real interoperability between equipment supplied by different vendors is achieved.

RFID seems to be in the middle of a major breakthrough depending on the ongoing work of global standardisation as well as the price of an RFID tag which continues to drop approaching the magic 5 cent limit of the bar code. Areas of usage are overwhelming, but there will be a period of time where only the most competitive and promising applications will prewail granting return on investment for critical investors. This is a technology in rapid change and the term "recent research" will have to be considered carefully as the picture might change from one week to another

3. RFID Standardisation

In this chapter we will look into what work is done on standardisation regarding RFID. The development of standards are very important for industry and others. ISO says the following about the importanse of standards in the introduction on their Home page [14] "*ISO standards contribute to making the development, manufacturing and supply of products and services more efficient, safer and cleaner. They make trade between countries easier and fairer. They provide governments with a technical base for health, safety and environmental legislation. They aid in transferring technology to developing countries. ISO standards also serve to safeguard consumers, and users in general, of products and services - as well as to make their lives simpler*".
Based on this statement one could agree that standardisation is very important to establish a common baseline for industry to make systems interoperable.

3.1 Standardisation organisations

3.1.1 International Standardisation Organisation (ISO)

ISO is a network of the national standards institutes of 148 countries. There is one member for each country. The Central Secretariat is coordinating the work in the organisations. The Central Secretariat is located in Geneva in Switzerland. The members are not official delegations of national governments and thereby a non-governmental organisation.

ISO have several activities on standardisation relating to RFID systems. In the ISO technical programme the following main groups are working with standardisation in relation to RFID. Interesting committees would be the following:

Joint Technical Commettee (JTC) 1 – Information technology
JTC1/Sub Committee (SC) 17 – Cards and personal identification
JTC1/SC31 – Automatic identification and data capture techniques
Technical Committee (TC) 23/SC19 – Agricultural electronics
TC104 – Freight containers
TC104/SC4 – Identification and communication
TC204 – Intelligent transport systems

Joint Technical Committee 1 on Information Technology

JTC 1 is a joint cooperation between ISO and International Electrotechnical Commission (IEC) [71]. The JTC 1 has two subcommittee that has developed standards concerning RFID. These two are subcommittee 31 (SC 31) and subcommittee 17 (SC 17).

JTC1/SC 31 - Automatic identification and data capture techniques

SC 31 are working with standardisation of data formats, data syntax, data structures, data encodeing and technologies for the process of automatic identification and data capture. SC31 has 4 working groups and working group 4 is called Radio frequency identification for item management. Each programme have developed a set of standards and are also working on new standards. On the ISO Home page there are comprehensive information on existing standards and on ongoing work in standardisations. When looking for a standard you can make a search on the web site and find the description for that specific standard. Also the information on the status of the standards can be found. ISO have develolped a system with status codes that details the current stage the standard has.

Table 4 - International harmonised stage codes [15]

STAGE	SUB-STAGE						
	00	20	60	90 Decision			
	Registration	Start of main action	Completion of main action	92 Repeat an earlier phase	93 Repeat current phase	98 Abandon	99 Proceed
00 Preliminary stage	00.00 Proposal for new project received	00.20 Proposal for new project under review	00.60 Review summary circulated			00.98 Proposal for new project abandoned	00.99 Approval to ballot proposal for new project
10 Proposal stage	10.00 Proposal for new project registered	10.20 New project ballot initiated	10.60 Voting summary circulated	10.92 Proposal returned to submitter for further definition		10.98 New project rejected	10.99 New project approved
20 Preparatory stage	20.00 New project registered in TC/SC work programme	20.20 Working draft (WD) study initiated	20.60 Comments summary circulated			20.98 Project deleted	20.99 WD approved for registration as CD
30 Committee stage	30.00 Committee draft (CD) registered	30.20 CD study/ballot initiated	30.60 Comments/ voting summary circulated	30.92 CD referred back to Working Group		30.98 Project deleted	30.99 CD approved for registration as DIS
40 Enquiry stage	40.00 DIS registered	40.20 DIS ballot initiated: *5 months*	40.60 Voting summary dispatched	40.92 Full report circulated: DIS referred back to TC or SC	40.93 Full report circulated: decision for new DIS ballot	40.98 Project deleted	40.99 Full report circulated: DIS approved for registration as FDIS
50 Approval stage	50.00 FDIS registered for formal approval	50.20 FDIS ballot initiated: *2 months*. Proof sent to secretariat	50.60 Voting summary dispatched. Proof returned by secretariat	50.92 FDIS referred back to TC or SC		50.98 Project deleted	50.99 FDIS approved for publication
60	60.00		60.60				

Publication stage	**International Standard under publication**		**International Standard published**				
90 Review stage		**90.20 International Standard under periodical review**	**90.60 Review summary dispatched**	**90.92 International Standard to be revised**	**90.93 International Standard confirmed**		**90.99 Withdrawal of International Standard proposed by TC or SC**
95 Withdrawal stage		**95.20 Withdrawal ballot initiated**	**95.60 Voting summary dispatched**	**95.92 Decision not to withdraw International Standard**			**95.99 Withdrawal of International Standard**

The table below has hyperlinks to the ongoing work on standardisation for each of the relevant committees.

Table 5 - Overview of where to find information on ongoing standardisation

Committee	Information
JTC1/SC31	http://www.iso.ch/iso/en/stdsdevelopment/techprog/workprog/TechnicalProgrammeSCDetailPage.TechnicalProgrammeSCDetail?COMMID=156
JTC1/SC17	http://www.iso.ch/iso/en/stdsdevelopment/techprog/workprog/TechnicalProgrammeSCDetailPage.TechnicalProgrammeSCDetail?COMMID=64
TC23/SC19	http://www.iso.ch/iso/en/stdsdevelopment/techprog/workprog/TechnicalProgrammeSCDetailPage.TechnicalProgrammeSCDetail?COMMID=999
TC104/SC4	http://www.iso.ch/iso/en/stdsdevelopment/techprog/workprog/TechnicalProgrammeSCDetailPage.TechnicalProgrammeSCDetail?COMMID=2904
TC204	http://www.iso.ch/iso/en/stdsdevelopment/techprog/workprog/TechnicalProgrammeTCDetailPage.TechnicalProgrammeTCDetail?COMMID=4559

3.1.2 International Telecommunications Union (ITU)

ITU is and international organisation consisting of members from both governments and the privtate sector. ITU is build up by three main sectors, the Radiocommunications Sector (ITU-R) [16], Telecommunication Standardisation Sector (ITU-T) [17] and the

Telecommunication Development Sector (ITU-D) [18]. There are currently 189 member states, 645 sector members and 94 sector accosiates. All sectors work through conferences and meeting. It is on these conferences and meeting that the members negotiate the agreements. ITU works with the principle of consensus-building. To carry out the technical work which lead to ITU recommendation Study Groups are made up with participating experts drawn from all member states and sector members and associates. The following text taken from the Home page of ITU describes what tasks the 3 sectors of the Union perform:

"ITU-R draws up the technical characteristics of terrestrial and space-based wireless services and systems, and develops operational procedures. It also undertakes the important technical studies which serve as a basis for the regulatory decisions made at radiocommunication conferences.
In ITU-T, experts prepare the technical specifications for tele-communication systems, networks and services, including their operation, performance and maintenance. Their work also covers the tariff principles and accounting methods used to provide international service.
ITU-D experts focus their work on the preparation of recommendations, opinions, guidelines, handbooks, manuals and reports, which provide decision-makers in developing countries with `best business practices' relating to a host of issues ranging from development strategies and policies to network management."

We are not aware of any specifications produced by ITU specifically for RFID.

3.1.3 The European Telecommunications Standard Institute (ETSI)

ETSI is an independent non-profit organisation producing telecommunication standards. It has 699 members from 55 countries.

ETSI ERM is responsible for standardisation related to electromagnetic compatibility and radio spectrum matters and has formed several Task Groups (TG)to work on standardisation. Relevant TG on RFID are:

- TG34 – RF Identification Devices
- TG28 – Generic short-range devices
- TG29 – Road Transport & Traffic Telematics
- TG37 – Intelligent Transport Systems

Relevant standards regarding RFID are summarised in the table below, but more comprehensive information can also be found on the Home page [19] :

Table 6 - Some relevant harmonised ETSI standards

ETSI Standard	Description	RFID specific
ETSI EN 300 220-1	Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment to be used in the 25 MHz to 1 000 MHz frequency range with power levels ranging up to 500 mW; Part 1: Technical characteristics and test methods	
ETSI EN 300 220-2	Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment to be used in the 25 MHz to 1 000 MHz frequency range with power levels ranging up to 500 mW; Part 2: Supplementary parameters not intended for conformity purposes	
ETSI EN 300 220-3	Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment to be used in the 25 MHz to 1 000 MHz frequency range with power levels ranging up to 500 mW; Part 3: Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive	
ETSI EN 300 330-1	Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment in the frequency range 9 kHz to 25 MHz and inductive loop systems in the frequency range 9 kHz to 30 MHz; Part 1: Technical characteristics and test methods	
ETSI EN 300 330-2	Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment in the frequency range	

	9 kHz to 25 MHz and inductive loop systems in the frequency range 9 kHz to 30 MHz; Part 2: Harmonized EN under article 3.2 of the R&TTE Directive	
ETSI EN 300 440-1	Electromagnetic compatibility and Radio spectrum Matters (ERM); Short range devices; Radio equipment to be used in the 1 GHz to 40 GHz frequency range; Part 1: Technical characteristics and test methods	Annex C Power limits for RFID systems operating in the 2,45 GHz ISM band
		Annec D Example of implementation for restriction of 4 W RFID to in-building use only
ETSI EN 300 440-2	Electromagnetic compatibility and Radio spectrum Matters (ERM); Short range devices; Radio equipment to be used in the 1 GHz to 40 GHz frequency range; Part 2: Harmonized EN under article 3.2 of the R&TTE Directive	4.3 Power limits for 2,45 GHz RFID systems

3.1.4 Uniform Code Council (UCC)

In 1974 UCC [20] founded the Universal Product Code. UCC is working for establishing multi industry standards for product identification and other related electronic communication. The goal is stated to be the enhancement of supply chain management and therby contribute to added value to the customer. UCC is a member organisation of EAN International

3.1.5 EAN International

EAN International [21] is an international organisation working on development of standards for uniquely identifying of products, shipping units, assets, locations and services. There are currently 92 member representing 94 countries. The representation from North America is UCC. EAN International and UCC has signed an agreement for the deveopment of a unique world wide system, the EAN.UCC system [22].

EAN International are managing the EAN numbers world wide with the exception of United States and Canada where UCC is allocating numbers. Example of EAN bar codes:

EAN-8 Symbol **EAN-13 Symbol**

3765 4320

4 512345 678906 >

Figure 12 - Example of EAN bar code structure

3.1.6 Electronic Product Code global (EPCglobal)

EPCglobal [23] is an organisation working with standardisation of RFID products. It is a joint venture between EAN International [21] and the Uniform Code Council (UCC) [20]. It is a so called a not-for-profit organisation working to establish and to support the Electronic Product Code (EPC) Network as the global standard for identification of any item in the supply chain of any company throughout the world.

The EPC Network technology has been devloped by the Auto-ID Center which was a partnership between alomost 100 global companies and five of the world's leading research Universities, the Massachusetts Institute of Technology in the US, the University of Cambridge in the UK, the University of Adelaide in Australia, Keio University in Japan and the University of St. Gallen in Switzerland. Together they defined a set of specification to use RFID in the supply chain management. The Auto-ID Center was officially closed on 26 October 2003 and the technology was transferred to EPCglobal.

EPCglobal has recently published the first version of their "Standards Developments Process" [24]. This document describes the process on how to get standards agreed with the EPCGlobal community.

At the EPCglobal Summit from 16 to 18 March 2004, EPCglobal announced [25] that two major companies joined the EPCglobal Board of governors. This was the CPC giant Johnson & Johnson and which are going to be the head of EPCglobals healthcare bord. The second company was Hewlett-Packard, which are going to be the head of the high-tech group. This is very important for creadability for EPCglobal and will further strenghthen their position. Microsoft announced [26] recently that they have become a member of EPCglobal.

Specifications

The specifications are currently version 1.0 and is listed in the table below. For each specification hyperlinks are provided.

Table 7 - Summary of current EPCglobal standards [27]

EPC Tag Data Specification	EPCglobal published a Proposed Recommendation for Review. People are invited to review and comment the version 1.1 of the EPC Tag Data Specification. The dead line for comments were 10 March 2004.. The specification will define the general data structure and the format of an EPC tag.
900 MHz Class 0 Radio Frequency (RF) Identification Tag Specification.	Specifies the communications interface and protocol for 900 MHz Class 0 operation. It includes the RF and tag requirements and provides operational algorithms to enable communications in the band
13.56 MHz ISM Band Class 1 Radio Frequency (RF) Identification Tag Interface Specification.	Defines the communications interface and protocol for 13.56 MHz Class 1 operation. It also includes the RF and tag requirements to enable communications in the band
860MHz -- 930 MHz Class 1 Radio Frequency (RF) Identification Tag Radio Frequency & Logical Communication Interface Specification.	Specifies the communications interface and protocol for 860-930 MHz Class 1 operation. It includes the RF and tag requirements to enable communication in the band.
Reader Protocol.	Defines the communications messaging and protocol between tag readers and EPC compliant software applications, including Savant.
Savant Specification.	Defines the services Savant performs for application requests within the EPC Network.
Physical Markup Language (PML) Core Specification, Extensible Markup Language (XML) Schema and Instance Files.	The PML Core specification established a common vocabulary set to be used within the EPC Network. It provides a standardised format for data captured by

	readers. It also includes XML Schema and Instances files for reference.
Object Name Service (ONS) Specification.	Specifies how the ONS is used to locate authoritative meta-data and services associated with a given Electronic Product Code.

Ongoing work on standardisation

They also announced [28] that they are going to publish a new draft standard during the summer of 2004. This standard will be the the standard called Class 1 Generation 2 which will be an UHF standard with more reliable read rates and better read ranges. They state that they are planning to submit this standard into the ISO standardisation process.

3.1.7 Automatic Identification Manufacturers (AIM)

AIM [29] is the trade association for the Automatic Identification and Data Collection (AIDC) industry. There are 17 member companies from the USA and one from Taiwan. They are dealing with many different technologies such as bar code, biometrics, electronic article surveilance (EAS), machine vision, magnetic stripe, optical character recognition, optical cards, RFID, radio frequency data communications, smart cards, touchc memory and voice recognition. One member that we know manufactures many different RFID products are Texas Intruments Incorporated. AIM is planning to conduct a Knowledge & Networking Forum in Brussels on 25 – 26 May 2004 [30]. The Forum will have focus on latest developments in the AIDC industry which mainly comprises use of RFID technology.

4. Radio Regulations

In this chapter we will provide information on radio regulation affecting the use of RFID applications.

4.1 ITU – Radiocommunication Sector (ITU-R)

The Radiocommunication Sector [16] is responsible for the managing of the Radio Regulations. The regulations apply to frequencies ranging from 9kHz to 400GHz and incorporate over 1000 pages of information describing how the spectrum may be used and shared around the globe. The complete list of services and frequency bands allocated in different regions forms the Table of Frequency Allocations, which is itself part of the Radio Regulations.

The ITU-R develops and adopts the Radio Regulations which is a set of rules that serve as a binding international treaty governing the use of the radio spectrum. It also maintaining the Master International Frequency Register. The regulations apply to frequencies ranging from 9kHz to 400GHz and contains more than 1000 pages of information detailing how the spectrum may be used around the world. Within the regulations it is a table called Table of Frequency Allocations. This table provides the complete overview of the services and frequency bands which have been allocated in the world.

The table of frequency allocations specifies that the following bands:

Table 8 - Information of ISM frequency bands from ITU Radio Regulations [31]

13 553 – 13 567 kHz	With centre frequency of 13 560 kHz
26 957 – 27 283 kHz	With centre frequency of 27 120 kHz
40.66 – 40.70 MHz	With centre frequency of 40.68 MHz
902 – 928 MHz	In region 2 (America) only, with centre frequency of 915 MHz
2 400 – 2 500 MHz	With centre frequency of 2 450 MHz
5 725 – 5 875 MHz	With centre frequency of 5 800 MHz
24 – 24.25 GHz	With centre frequency of 24.125 GHz

are also designated for ISM applications. Therefore non-ISM radiocommunication services operating within these frequency bands will have to accept the harmful interference which may be caused by the ISM applications.

4.2 The European Conference of Postal and Telecommunications Administrations - CEPT

What CEPT [5] is can best be described by themselseves. Taken from the Home page of CEPT: "*The European Conference of Postal and Telecommunications Administrations - CEPT - was established in 1959 by 19 countries, which expanded to 26 during its first ten years. Original members were the incumbent monopoly-holding postal and telecommunications administrations. CEPT's activities included co-operation on commercial, operational, regulatory and technical standardisation issues.*
In 1988 CEPT decided to create ETSI [6], *The European Telecommunications Standards Institute, into which all its telecommunication standardisation activities were transferred. In 1992 the postal and telecommunications operators created their own organisations, Post Europe and ETNO respectively. In conjunction with the European policy of separating postal and telecommunications operations from policy-making and regulatory functions, CEPT thus became a body of policy-makers and regulators. At the same time, Central and Eastern European Countries became eligible for membership of CEPT. With its 45 members CEPT now covers almost the entire geographical area of Europe*."

Originally 3 committees was established, one for postal matters, CERP (Comité européen de Réglementation Postale) and two on telecommunications issues: ERC (European Radiocommunications Committee) and ECTRA (European Committee for Regulatory Telecommunications Affairs). The committees handle harmonisation activities within their respective fields of responsibility, and adopt recommendations and decisions. These recommendations and decisions are normally prepared by their working groups and project teams. In September 2001 the ERC and ECTRA merged and the committee called Electronic Communications Committee (ECC) was created. It is the ECC that is dealing with RFID issues. More specifically, it is the Short Range Devices Maintenance Group which is responsible to maintain and update the ERC REC 70-03 [32]. News and information can be accessed on their Home page [33].

The ERC REC 70-03 document is relating to the use of short range devices and contain the following:

Table 9 - List of appendixes and annexes of ERC REC 70-03 [32]

Appendix 1	Applications and Parameter Tables
Appendix 2	List of relevant ERC Decisions, Recommendations and ETSI Standards
Appendix 3	List of national restrictions
Annex 1	Non-specific Short Range Devices
Annex 2	Devices for Detecting Avalanche Victims
Annex 3	Wideband Data Transmission systems and

	HIPERLANs
Annex 4	Automatic Vehicle Identification for Railways (AVI)
Annex 5	Road Transport & Traffic Telematics (RTTT)
Annex 6	Equipment for Detecting Movement and Equipment for Alert
Annex 7	Alarms
Annex 8	Model Control
Annex 9	Inductive applications
Annex 10	Radio microphones
Annex 11	RFID
Annex 12	Ultra Low Power Active Medical Implants
Annex 13	Wireless Audio Applications

Annex 11 is specifying RFID but other annexes are also relevant for RFID applications. Especially Annex 1 – Non-specific Short Range Devices, Annex 5 - Road Transport, Annex 6 – Equipment for Detecting Movement and Equipment for Alert and Annex 9 - Inductive applications.
What parts and which countries that have implemented the ERC REC 70-03 is listed in a document called: Implementation of ERC REC 70-03 [34] and is dated 14 april 2004.
Also news an update on activities for the Short Range Devices Management Group can be found on the Home page of the European Radiocommunications Office (ERO) [35]

4.3 European Parlament and the Council

The European Parliament and the Council has issued directives [36] (proposed by the European Commission) regarding regulatory issues for electronic communications. The Directive 2002/21/EC issued on 7 March 2002 on a common regulatory framework for electronic communications networks and services details specifically in article 9, the Management of radio frequencies for electronic communications services. This article also refers to a EC Decision which in more detail is about radio spectrum policy in the European Community. This is the Decision No 676/2002/EC of 7 March 2004 [37] on a regulatory framework for radio spectrum policy in the European Communicy (Radio Spectrum Decision). It states that the member countries should continue to work within the CEPT and ITU World Radiocommunications Conferences to ensure that the European Community's interest are being taken into account. The aim is to establish a policy and legal framework in the European Community to ensure the coordination of policy approaches to establish efficient use of the radio spectrum.

The European Commission and CEPT

On 30 January 2004 [38] the European Commission and the European Conference of Postal and Telecommunications Administrations (CEPT) signed a Memorandum of Understanding (MoU) with the aim to foster a contructive collaboration in areas of common interest. They state that their joint activities are expected notably to help European citizens to benefit from new wireless technologies and products.

ECC gives the information at the new listing on its Home page [33] that the EC has also given a new Mandate on Short Range Devices. Among several specific objectives the Commission want to increase both the number og Short Range Device categories and the frequency ranges of Class I equipment under the R&TTE Directive 1999/5/EC [39], take into consideration the benefits of identifying bands for generic SRD usage instead of for specific applications, and provide additional harmonised bands to emerging types of SRDs and need evolve. The target date for CEPT to provide the final report to the Commission is 15 November 2004.

4.4 Regulation in the USA

In the USA the regulatory responsibility of the radio spectrum is divided between two agencies. The Federal Communications Commission (FCC) [40] is responsible for the non-Federal government use of the spectrum and the National Telecommunications and Information Administration (NTIA) [41] is responsible for the government use. In the USA the frequency spectrum from 9kHz to 300 GHz is regulated. For international harmonisation the FCC and NTIA assist [42] the Department of State when working within ITU. The previously mentioned ITU's Table of frequency allocation is reproduced in the FCC's Table of Frequency Allocations. The table can be found on their Home page [43].

4.5 National regulation

For Norway, which we are located in, regulations regarding use of frequencies are in force. The regulation called Authorised Frequency Use [44]. The Regulation assigns frequencies on specific terms based on the principle of general authorisations (licence exemptions). It is dated 20 Dec 2000 with no 1399 and is approved by the Norwegian Post and Telecommunications Authority [45].

For the EAS-applications using accoustic waves there are no restrictions if using frequencies belov 9kHz. (Section 5). Section 9 details frequencies and restrictions regarding emitted power for various short range devices. Section 10 details use of Radio equipment for detecting movement for frequecy bands 2.4 – 2.4835 GHz, 10.5 – 10.6 GHz, 24.05 – 24.25 GHz, 9200 – 9500 MHz, 9500 – 9975 MHz and 13.4 – 14.0 GHz.
Section 19 details use for Inductive systems:

Table 10 - Inductive systems

Frequency band	Maximum authorised field	At distance
9 – 59.750 kHz	72 dBm A/m	10 meters
59.750 – 60.250 kHz	42 dBm A/m	10 meters
60.250 – 70 kHz	72 dBm A/m	10 meters
70 – 119 kHz	42 dBm A/m	10 meters
119 – 135 kHz	72 dBm A/m	10 meters
6.765 – 6.795 MHz	42 dBm A/m	10 meters
7.4 – 8.8 MHz	9 dBm A/m	10 meters
13.553 – 13.567 MHz	42 dBm A/m	10 meters
26.957 – 27.283 MHz	42 dBm A/m	10 meters

Section 22 details Radio frequency identification equipment in the 2446 – 2454 MHz frequency band. Section 22 states that the frequencies should be used as detailed in Annex 5. This is an error and should be Annex 11 which is about RFID. The Norwegian Post and Telecommunication Authority is aware of this error and it will be corrected, the next time the legislation is being updated.
If you are using RFID applications in Norway which operates within the authorised field values and withing the limitations of radiated power the frequency bands specified can be used for free without paying any regulatory fees.

5. Ethical, Privacy and Security Considerations

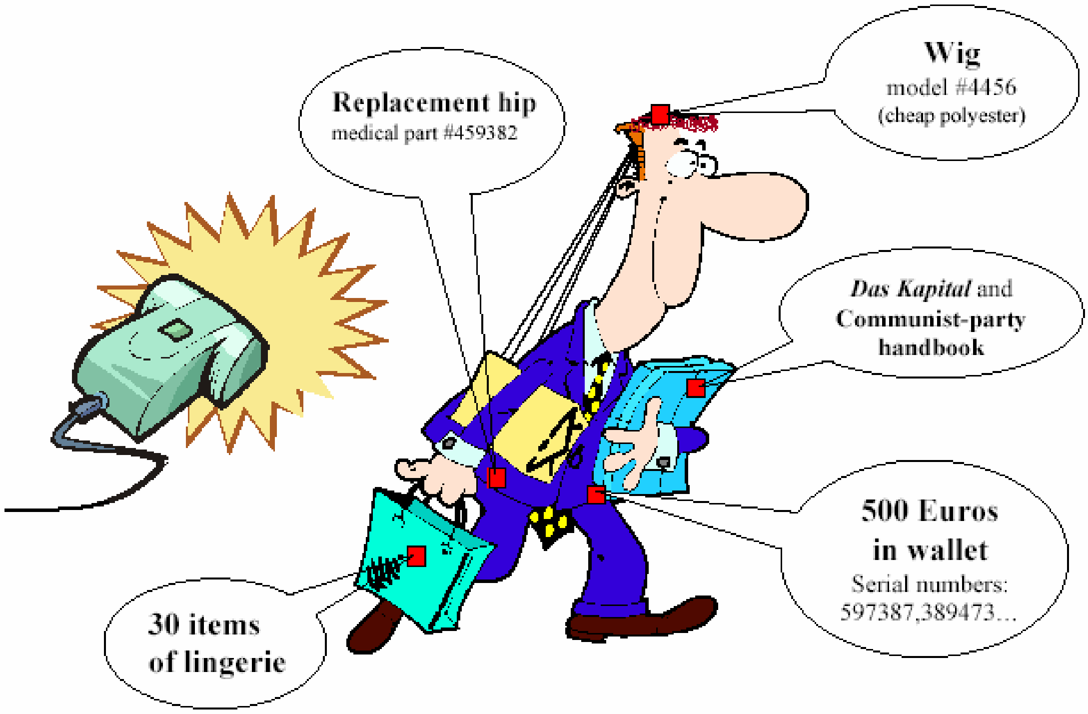

Figure 13 - RFID will be everywhere in the future [46]

5.1 Ethics

There are numerous reasons for applying RFID in emerging business or industrial applications. The ability to perform "around the clock" monitoring of any object, people included, leaves a frightening perspective of what could be, unless we implement mechanisms to deal with ethics along the way. Keeping track of objects on the move or keeping inventory should be a good thing making everyday life easier for business or system owners. In many cases, it is considered to be a good thing, but the problems arise when the collected information can be used for other, and often unintended, purposes as well. RFID wristbands can hold personal information about hospital patients thus reducing the risk of entering wrong information related to blood samples and other tests being taken of the patient during his or hers stay at the hospital. In a Big Brother perspective, this information could easily be used to track the patients as they move around within the hospital by placing electronic gates by the doors of interest. Although useful, this information was not intended to be statistics in a survey in the first place and the patients might not know that they are being monitored either. Marking every consumer article with a tag will, when read at the till, leave the producer with, for him, valuable information representing consumer statistics. RFID in retail was meant to record when shelves were empty and refilling required. Obviously, we will need a code of ethics to prevent information collected for one purpose from being exploited, especially those serving as a tool, for measuring the economical success of a product or a service. There is a thin line separating the and good intentions of an RFID applications from the potential exploitations of the very same example. In a way ethics is a means of protecting the consumer privacy from being corrupted, as the case would be when individuals are being tracked without their knowledge or consent.

5.2 Privacy

Dealing with the use and deployment of RFID technology are quickly moving from business needs to political decisions. Technologists have created remote identification technology, but the question is if the public want it. Last year, Benetton withdrew its plan to put RFID chips into some clothing after activists garnered international attention by pointing out that Benetton was about to deploy a technology without thinking through the privacy implications. [47]

“Privacy has always been a strong value and concerns over the perceived invasion of privacy, whether justified or not, is a factor that must be considered in any RFID rollout. As with many technological advances, early concerns often stem from a lack of understanding of the technology and its capabilities.” Is bying a RFID tagged sweather an opportunity for others to track you and your piece of clothing around the globe?” [48].

When RFID becomes a part of everyday life it is not very difficult to se that the information provided by RFID tags can be exploitet and could be a threat to consumer privacy. If all your clothes were tagged someone with a RFID reader could find out exactly what kind of clothes you were wearing. Also the content of bags and handbags could be read by other people and be exploited. If the name of the consumer where stored after each perchase an exact RFID id for each product could be stored. If this information fell into wrong hands it could be exploited in many different ways. A person could be tracked by searching for a unique RFID tag id in any product he had purchased. If readers were positioned at strategic places like train station, airports, bus stations and connected to a central computer basically everyone could be tracked everywhere. This would be a violation of a persons privacy an illegal in most countries.

Currently when RFID tags are used in EAS systems the tags are either removed or destroid before the customer leaves the shop. Because the tag is no longer active it poses no threat to the consumers privacy. The problem raises when the RFID tag is still active after the consumer has left the shop. For developing new innovative applications it would be absolutely vital to have an active RFID tag in the products. Also it is expected that the RFID would sooner or later take over for the use of bar codes. When this happens, methods to protects consumer privacy must be in place.

Various proposals have been made on how to solve this problem which is vital to be solved for the RFID applications to evolve in the future. One promising proposal comes from Ari Jules and Michael Szydlo both at RSA laboratories and Ronald L. Rivest at Laboratory for Computer Science, MIT. The solution is called “The Blocker Tag” [49].

The Blocker Tag

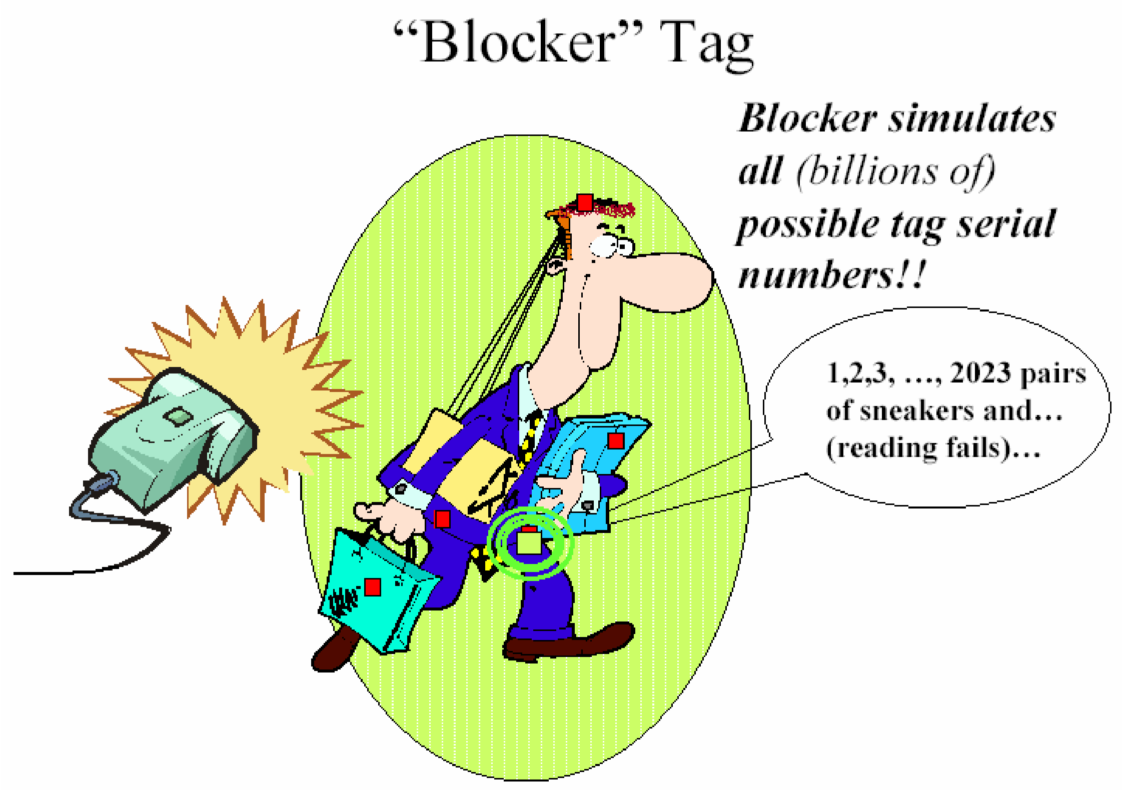

Figure 14 - Blocker tag concept [46]

As the title says the blocker tags idea is to block the response from a tag after a query from a RFID reader. By blocking the RFID tags to respond, access to them is prevented and thereby the privacy of the person carrying the actual tag is protected. The concept of the Blocker Tag is to exploit the characteristics of the Tree-Walking Singulation Protocol which is used for systems that must be able to access several tags within a readers coverage area. The tree-walking sigulation algoritm eanbles the RFID-tag reader to idenfity the serial numbers of nearby tags individually by means of a bit-by-bit query process resembling a depth-first search of a binary tree. The basic principle for the blocker tag is to force the reader to try to located tags within the whole range of serial numbers. For the simlest tags the serial number is of the magnitude of 64 and therefore the reader has to search for 2 in 64 to locate all tags. This will of course take too much time and the reader will be unable to read any tags.

5.2.1 Legislation and regulation regarding privacy

USA
In the USA you have The Privacy Act of 1974 [50], which details restrictions regarding handling privacy issues.

Europe
EU has issued a Directive dealing with protection of individuals. This is called: "Directive 95/46/EC [51] of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data". Which countries that have implemented this Directive can be found on the European Commission Home page [52].

In Norway, The Data Inspectorate [53] is responsilbe for enforcement of the Personal Data Act of 2000 [55] and the additional regulation [56]. This act has been harmonised with Directive 95/46/EC. [51] The Inspectorate is an independent administrative body under the Norwegian Ministry of Labour and Government Administration. In their report on protection of privacy from 2004 [54] they are talking about the potensial risks with RFID. They state that using RFID tags on Hospital personell and patient could only be accepted in special cases. The possilble exploitation when using RFID for the Toll Road system and in clothes are also mentioned. They state that they will moitor the situation closely and pay attention to the development in this area.

5.3 Security

When using RFID in security systems and for payment and ticketing, a certain degree of security would be required. For other applications, and still not discovered applications, you would need security features with your RFID systems. You would not want the data on a RFID tag to be read and duplicated and in that way give unauthorised access to a building. If the Toll Road RFID tags could be copied and misused, it would be a serious matter. Also in some cases the transmission between the tag and the reader are of such a nature that an unauthorised user should not get hold of the information. Eavesdropping can therefore be prevented by using cryptografic functions.

Security concerns
Any system based on wireless communication is vulnerable to eavesdropping, access by unauthorized users and intrusion of priacy or malicious attacks due to unprotected transmissions of sensible information as the case might be in hospitals or banking environments. Non line of sight communication is often featured as one of RFID's greatest benefits over barcodes. On the other hand this could be an additional drawback as direct galvanic contact and "eye" contact with the reading device leaves the user in better control of the communication process not beeing compromised by others. Until

now there has been an increasing quest for cheaper tags, leaving less room for security concerns. Certain applications will have to put more focus on security than others, in order to reduce the risk of beeing exposed to security threats and the harm they might cause to the system owner. Alternative mechanisms are encryption and authentication.

Encryption

Each and every tag has a unique identity which is established during the production process. In general anyone can read this identity by using equipment with the same system parameters and operating on the same frequency. The matter gets even more serious if someones identity is linked to this tag as the case might be for patients in a hospital wearing a RFID wristband for easy identification. What if someone is tracing these patients to make a survey on their wherabouts? This would definately be very interessting information for insurance companies. Another scenario is consumers carrying whatever they bought for the weekend in a number of bags. By scanning RFID marked articles from a distance one would, over time, be able to draw a pretty good picture of their consumer habits. This is often called leakage of consumer data without the user beeing aware of this tapping. This could be prevented by encrypting the transmission from tag to reader.

Authentication

A necessity in systems handeling ticketing or payments where a high level of security is required. A possible scenario is where false datacarriers or tags are used in an attempt to fraud the company in question. A related case would be to place false readers in an attemt to access information stored on legal / valid data carriers. Two measures are often used to avoid this from happening. These are mutual symmetrical authentication and by the use of derived keys techniques. In the first case both tag and reader share a “secret key” as described in ISO 9798-2. This solution is not well suited for systems comprising millions of tags as the risk og generating two identical keys would increase and so would the possibility for compromising the key. When using derived keys however, the reader uses the vendor dependent serial number of the tag. By the use of this number and a master key the authentication key of the transponder is calculated. This procedure often takes place in a special SAM (Security authentication module) module located on the reader.

6. RFID Applications

6.1 Main Sample Applications

The basics of the RFID technology was presented in chapter 2. With this in mind it is time to put focus on the practical implementations of the RFID technology over the last decades. In this chapter we will provide exsamples of some existing RFID applications. There are numerous applications taking advantage of the benefits offered by the RFID technology. This is partly due to the increasing focus and attention that has been brought onto wireless communication recent years. Many of these can certainly be characterised as experimental and thus never be fully commercialized. On the other side there are a number of applications that were established in the 60-70's that has proved themselves solid and lifeworthy even for future use. In the following there will be an overview of the most common RFID applications. Some of these are even given a new boost due to cheaper tags, added functionality or both.

6.1.1 Manufacturing - Industrial Automation

An assembly line where processes and stages along the conveyorbelt are documentet and tested due to machinery that's able to read information about the item in question as it passes on the line.

Industrial production
This scenario also originates from the introduction of the conveyorbelt allowing industrial massproduction to take place. Numerous machines along the line are specialized in performing one operation or producing one part of the product. In the case where a specified part is not produced the opertion may consist of a robot painting a part or functional testing of the product along the way. In order for this to take place each single product must be identified. Next status must be registered from station to station allowing measures to be taken if a faulty product is present. Individual marking of the parts has this far been done by the use of barcodes allowing laserreaders to identify the parts as they pass the station on the conveyorbelt. This picture obviously appeals to the RFID technology as one no longer would depend on free line of sight and correct angles for reading. Nor would dirty labels as a result of gases, paint or oil as well as moist. The most promising advantage would still be the opportunity to even write information to the tags representing status for the specific part after passing the station in question. This technology is especialy applicable to the car industri where series of one model often are delivered in different colours, with different equipment, enginealternatives and so on. By letting robots reading the "car recipee" in the shape of a RFID tag, they would instantly know how to treat the next chassis coming up on the production line.
To summarize the advantages are numerous and among the most obvious are:

Quality control as the last station of the productionline would be able to read the total status of the object in one single operation gathering all information collected along the conveyorbelt.
Security as changes in the product data can be electronically distributed from a central computer to the associated station. This could eliminate a large lot of faulty production as corrections can be carried out along the way.
Data security would be a necessity as error detecting and correcting codes provides little risk of data errors due to errors occuring in the transmission from host to station.
Flexibility as customized objects can be made down to one single object as batch programming from the central computer towards the robots will no longer be necessary as the “blueprint” of the object is hold in the belonging tag.
Robustness as the weaknesses of the barcode will no longer require a clean production environment allowing moisture, fumes, gases, oils and high temperature to be present. Even the presence of dust will not influence on the readability of the tags as the requirement of free line of sight no longer applies.

6.1.2 Electronic Article Surveillance (EAS)

Examples are Checkpoint- or anti theft s systems often found in shops and stores. These are usually featuring simple1-Bit systems capable of detecting the precence of a tag, as the customer leaves the shop through an electronic gate featuring the reader. One case would be that the tag has not been removed by the till implying that the merchandise has not been paid for. Another variant is that the tag remains on the paid article yet the alarm is not triggered as the capacitor across the antenna circuit is destroyed in an operation performed by the operator at the till, preventing the tag from responding to the reader signal. This is also called deactivation of the tag and will in most cases destroy the tag permanently. Still there are systems offering reactivation of deactivated tags.

6.1.3 Security Applications

Access control

By physical or non physical contact with the reader enabling access to restricted areas, buildings and so on due to preprogrammed information on the tag. This application can be split up in two separate areas which are on- and offline systems:

Online systems

This solution is characterised by the fact that a large number of people are granted access at relatively few points of access. The typhical approach to this problem is a centralised computer connected to all the associated access points allowing the operator to edit the list of parameters that controls who is to have access at which point at which time and so on. The local access points are often realised by a reader and corresponding circuitry card containing a local database of the legal cardholders. An updated list might be downloaded from the central computer on a regular basis. Personal information about the cardholders should not be stored on the card as this information is availiable in the central computer and revealed as the identification number on the card is translated into a real identity.

Offline systems
As an alternative to online systems there is the situation where a small number of people need access to a large number of rooms. In this scenario each individual doorway will have to be equipped with a terminal of its own. There will be no network connecting the terminal to a centralised main computer thus no way of administrating the system from one central position. A local terminal placed at the door will contain/hold information of which persons are granted access to this particular doorway. Thus the cardholder will carry with him information about where he is allowed to pass. This information will be checked against the terminal and due to this access will be granted or denied. At a Hotel the keycard would typhically be programmed at the reception when the specific room is booked by the persons who will have access to the room for a limited period of time which in fact is another parameter to be handeled in the programming process. This concept is offering several advantages over conventional lock systems as lost keys could easily be deleted from the corresponding terminal. Staff could be equipped with keys programmed for access to last for as long as they are employed or for a limited amount of time. The immunity against dirt, wear and moisture comes very useful as the previous systems has suffered from malfunction due to these problems.

Electronic Immobilisation
One major application is within the car industry where more expensive cars are equipped with a wireless system which requires the presence of a tag or else the car will be impossible to start.

6.1.4 Ticketing

Baggage tagging is a mean to improve baggage handling at the airports as information of relevance can be written or read from the bags as they progress from the point of delivery to the airplane. This makes identification of luggage easy in the case where the owner has not entered the plane in due time and where it will have to be removed before the plane is allowed to leave.
This principle is also adopted by buscompanies all over the world as an improvement to systems who require cards to be inserted into a reader requireing galvanic contact in order to operate. The advantages are numerous including less cash availiable on the bus thus the chance of a robbery is reduced. Then there is less time wasted as the driver doesn’t have to issue tickets and change to the passengers.

6.1.5 Animal identification

One of the true classics among RFID applications is performing surveilance of live stock as well as allowing individual treatment by machinery i.g. milking machines is made possible as the reader recognizes each individual and can adjust according to the information stored in the tag. A system keeping track on animals in the fields could also be combined with GPS functionality allowing around the clock surveilance of each individual animal.

6.1.6 Toll Road Control

Offers various mechanisms to automate the process of passing a toll plaza without stopping due to a prepaid subscription. This information is programmed into a tag often fastened to the windshield of the car signalling to the reader as the car passes through the interrogation zone.

Norwegian AutoPass system

The use of RFID for toll road collection has been used in Norway for several years. In 1999 several systems used by the Norwegian Public road Administrations was uppgraded to use a system using 5.8GHz as detailed in ERC 70-03 Annex 5.

6.1.7 Supply chain management/Logistics

Asset tracking

RFID is beeing used by the postal system to track parcels through the process of delivery and sorting along the way. Benefits of the RFID technology are that items can be read without the concern of orientation and line of sight.

7. Research and Development Projects on new RFID Applications

In this chapter we are going to document what is going on within the area of research and development of new RFID applications. We will only be documenting enterprise applications.

7.1 Public Transport – automatic fare collection system

We have seen some applictions with automatic fare collection using smartcards. These have certain limitations. If we could start to use RFID tags and agree on standards it would be very benificial. Currently a common standards for toll road collection in Norway has been implemented. Maybe a common system for fare collection for public traffic could be implemented?

7.2 RFID Sensors

Detection of pathogens in food is another area of ongoing research. By doing this you would be able to prevent deceases and death caused by food poisoning. By integrating sensors on an RFID tag one would be able to detect harmful bacteria and toxins in food at an early stage.

Industrial scaling technologies and mass production has resulted in mineature tags with embedded sensortechnology capable of logging a number of measures over a wireless interface. In addition the concept does not depend on an onboard powersource making this an unique solution for a large number of applications. The obvious limitation to this scenario is the rather short range of operation associated with the passive option of operation. Yet a number of solutions remains. Closely related to this concept is the idea of whole network of sensornodes monitoring a given measure as pressure, heat, humidity, light or another relevant attribute.

7.2.1 Sensor networking, the pervasive internet and the automation of the global Enterprise

The major boost for the future internet might be the establishment of global sensor based networks highly specialised in harvesting information from numerous applications worldwide, taking advantage of the distributed memory and processor capacities of RFID equipped appliances. In other words the recent growth in users linking up with the internet is likely to be replaced by an ever bigger growth in internet adoption by non humans allowing devices and networks of devices to interact automatically without human intervention. “By the year 2010 the internet will have trillions of users it doesn’t have today. Most of them will not be human beings” ref?
The internet has obviously totally changed our perspective of global communications. Networks are growing bigger from one day to another and the Internet provides a way of

interconnecting networks across borderlines allowing a tighter integration of enterprises on a worlwide basis. Drivers boosting this tendency is the quest for connectivity, open standards and the urge to share information. This far human communication has been the major force behind the ongoing work. A new trend is the need for exchanging information between networks of machines representing a global networks of intelligent nodes that serves a number of purposes. A centreal idea is the automated enterprise based on machines and where the outposts of this automated neural network is represented by RFID readers capable of reading information from a tagged world. There are already numerous of gadgets offering communication as Bluetooth, WLAN, GSM and so on. Do we really need another box to carry around? We definitely don't as we associate the process of collecting information by a portable RFID reader to be rather cumbersome. One solution to the problem is to integrate the device into our most personal belongings. Nokia has already taken this step and the result is that information is automatically registered in a number of ways just as we move by equipping the mobile phone with a RFID transponder. In the same way just about anything could be equipped with a RFID tag in building a giant worldwide neural system of transponders. By applying this network just about any electronic device would be able to eastablish communication to the outer world making its content or memory availiable to potential users worldwide. Another proposed usage would be RFID sensors capable of registering measures as temperature, pressure or even the precence of agents in a war setting alerting the use of toxic gases. Harvesting this information represents the potential of making business far more efficient and economic and profitable and thus promising return on investment for investors. Harbor Research calls this phenomenon "The pervasive internet", the fusion of pervasive computing, internet connectivity, and new enterprise-level data management applications and web based smart devices. Another term used is "Invisible Business". As a result of this devices without the capability to communicate this way will loose much of their value compared to online units. A central part of this scenario is the RFID tag capable of performing live measurement of just about anything that can be measured or sensed. This feature allows the tagcarrying object to identify itself to a present reader which in turn will make the information availiable to potential users just about anywhere in the world. The tag could measure the temperature of the surroundings of a piece of ham, the pressure of an oxygene tank or the weight of cars passing a bridge. Associated applications could be supply chain management or logistics where the information mentioned could be monitored in real time offering tremendous advantages compared to conventional solutions. The fundamental idea is simply to allow an automated flow of information from one end user to another where an end user is represented by a device or an RFID tag rather then a human being.

7.3 Slaughterhouse Gilde – animal tagging

The company Gilde manufacturing food for consumers is currently doing resarch and devlopment projects [72] with RFID in Norway. In the western part of the country at Gol 90000 sheep are tagged every year to be able to control the animals movement all the way to the slaughterhouse. They state that they save several millions of Norwegian kroner every year because of the automated system with registration at the slaughterhouse. Also the farmers are getting a more secure system assuring payment for each sheep because the factor of human error has been eliminated. In another branch they are testing with RFID-tags on trays for identification. They stated that it is cost saving because they do not have to buy the bar code stickers and the glue. Also the functionality is improved. Bar codes tended to be impossilbe to read because of blod spill. With the RFID tags the trays can be identified regardless of blod spill..The company summarises the results so far by stating that the potensial for cost savings are big. The RFID system are tuned to their new ERP-system and reveils new possibilities for integration.

7.4 Identifying trailers with RFID tags

One implementation project [57] aims to tag up to 2000 trailers with unique RFID tags for quicker and more relaiable idenfication.
The system has been deployed at Paramount Farms which processes around 60 percent of the U.S. pistachio crop. 50 percent of the pistachios it sells comes from from a network of 400 partners from various growers of pistachio nuts. The new implemented system uses Microsoft's .Net technology and Microsoft SQL 2000 database for the main Grower Receiving System. The system was developed and imlemented by MagTech System. Information on the trailers's tare weight, licence plate number and owner information is stored in the database. When the trailer is placed on the scale where the RFID readers are located the unique RFID tag are read and the stored information in the database is retrieved. Then the the gross weight, date and time are stored to be able to track when each of the owners of the trailers delievered pistachio nuts.

Benefits
Measurement after the implementation has shown that the transaction time for initiating a new load has been reduced by 60 percent. Also data integration and accuracy have improved with the automated system. Before they had a manual system with possibilities for human error. The new system has also contributed with a better control over all the trailers enabling an optimised equipment sechduling with a reduction in trailer usage of 30 percent.
Other benefits experienced is that the grower partner are happy with the new system.
Also added benefits with using the information stored in the database to devlop new customer relation application has been thought of. One example is a planned web interface for the growers to access information about their own deliveries.

7.5 Tracking of containers in the Military supply chain

During the operation Iraq Freedom the US Military used RFID tags extensively to track containers shipped to the theatre of operations and the content of air shipment pallets.[58] The use was a big success in tracking supplies and material. During Operation Desert Storm in 1991 about 40000 containers were shipped to the theater. Half of them had to be opened and manually searched or inventoried in order to clarify the contents. Many of the containers were actually not opened at all. The massive inefficiencies experienced in 1991 caused the Department of Defence to look for other means of making the supply chain management more efficient. In some cases in Iraq the RFID was used in conjunction with GPS positioning to be able in real time to track containers. Otherwise, fixed or mobile RFID readers were deployed at airports, airfields, distribution centers and assembly areas to scan the RFID tags. When the RFID tags were interrogated the information such as tag ID, reader location and date-time-group were forwarded to a central server. The communication from the RFID reader were implemented in many different ways depenting on available infrastructure, including fixed phone line, mobile phone, satellite phones using Iridium, Internet or local intranett if available. There raw RFID data were then accessable for any supply offices through a web interface. They state that the current system is a specific product provided by one company. They are welcoming more standardisation to enable more competition with regard to bid for system contracts with the military.

7.6 Identification patients and blood samples at a hospital

Master students at Agder University College has documentet that RFID can be used to identify blood sample instead of bar codes used today [59]. The process how to handle the blood samples are described in the paper. One motivation factor for implementing a RFID system in this scenario could be to reduce the risks for human error. Before a system like this could be implemented, the automated analyzing equipment must be equippmed with a RFID reader instead of the existing bar code reader.

7.7 Identification of patients using RFID wristbands

In Iraq the US forces conducted trials with using RFID wristbands on patients at the military field hospital [60]. The soldiers were given wristband when arriving at the Pensacola Fleet Hosptial and the hosptal used the tags serial numbers to make a unique identification.

7.8 Tool inventory system

Establish zones of RFID readers to cover a large production area. Special tools could be scattered around if there are lack of proper procedures to put the tools at its place. All RFID readers are connected using WLAN to avoid putting cabling everywhere. A main application is then on a periodic basis polling all RFID readers to get a map of the production area where the all the tools are located.

7.9 Bus Tracking System

Example from Veilje in Denmark with tracking of buses in the city. At each stop you could have a reader and identify the bus as it passes the stop. At least you know where the bus was at the last stop.

7.10 RFID equipped mobile phone launced by Nokia

The feature with RFID equipped mobile phone by Nokia was revealed at the CeBIT happening in Germany earlier this year [61]. The concept is based on 13.56MHz technology allowing the owner of the mobile to read tags and get access to remote information by use of the reader. One of the ideas behind the launch is to enable guards and such working for security companies to sign for their presence at certain sites or buildings and to transfer this acknowledge of presence to be transffered to the main office by use of the GSM system. An option is to store the information locally and downloaded to a computer later on. This move seems to be part of a trend where readers that usually represents the stationary part of a RFID system are given the role of the mobile part. The reader is designed/shaped like a cover that can easily replace the orgininal cover following the phone at purchase. The software is written in Java by Nokias own pool of developers. The standard used for this purpose is the ISO 14443A and the read range is 2 – 3cm. The keyword for the overall use seems to be easiness for the end user who shouldn't have to be a technician to be able to operate the set. An interessting fact though is that by reading 50 – 80 tags a day, the battery is said to last for several days. This will surely be an alternativ way to operate or serve many of the eastablished RFID applications. Why not use your mobile as a ticket for the concert and download the appropriate code while you are on your way to the concert by bus?

7.11 Mapping and localization with RFID technology

Location context can provide important information for the interpretation for RFID readings. The marking of objects by RFID tags is applied [73] in a number of applications and this has come to point where the ability to combine the marked object with its location is the matter of interest. An automated system telling you that your car is stored in your garage is hardly considered as breaking news. If the system provides information about the movements of your stolen car on the roads of a foreign country, now that would be quite useful information. By adding information of object localisation RFID technology can be brought another step forward. Normally the RFID readers are fixed objects detecting the preence of a tag by emitting a radiation field. This is usually done by registrating the tags as the objects they are attached to passes through electronic gates, tills or other bottlenecs where people are likely to pass. An alternativ approach would be to allow moving readers to continuously scan the area of interest for tags. Specialised robots with on board reader would then be capable of making maps of RFID tags in the specified area. Equipped with two antennas a RFID-reader on an mobile plattform should be able to locate potential tags in its surroundings. Based on this a map could be produced allowing another robot to easily detect these objects later in a fraction of the time spent in the mapping phase. This concept could be adopted to trace objects on a global basis by the use of laser data. The idea behind the concept is simple enough. By keeping track of what items the persons or robots are touching valuable information can be gathered and processed for further knowledge within a specific field of interest.

7.12 System for automatic detection of expired food based on an on-board temperature sensor

Such a system would rely on a standardisation of food marking allowing different chains of suppliers to handle the same markingsystem. This would imply continious monitoring of the temperature the article has been exposed to during its lifecycle.

7.13 Tracking children in amusement park

Legoland in Denmak are going to offer a new service [62] to parents in their amusement park. The service cost 3 euros for one day’s rental and the parents can send and SMS message to locate their child. Withing 20 seconds they will get a response back with the location. Instead of traditional RFID tags and readers the system uses a combination of the 802.11b technology with RIFD technology. To be able to locate the tags they are using triangulation techniques and calculates the distance from the 3 nearest location receivers. The park has only purchased 500 tags but expect they will have to buy several thousand.

7.14 Tracking critically injured patients in hospital

In a research project [63] the company American Project Services has worked together with the University of Memphis’s FedEx Center for Supply Chain Management and the Shelby County Regional Medical Centers Trauma Emergency Department. They project is about tracking critically injured patients with RFID technology. Critical injured patients were equipped with RFID tags and they were able to track the patient using 25 RFID readers within the facility. The fist phase of the project was ended in April 2004 and the result was reported to be very promising. The representatives for the projects states that they tracked the patients with 100 percent accuracy. The tags were attached to the patients ancles. The project used tags and readers from Alien Technology operating in the ISM band at 2.45 GHz using active tags with reading range up to 30 meters. No patient data was stored on the tags. They only used the unique tag number to track each patient. The projects stats that they logged the patient position 40 to 50 times per minute and the information about the location was transferred via the local LAN and stored in an SQL database.

7.15 Asset tracking of medical equipment

Agility Healthcare Solution has made a new contract with three hospitals in Virginia. The intention is to manage mobile assets and enhance healthcare workflow and business proecesses using RFID technology [64]. The system will be able to locate and determine the exact location to all tagged medical equipment. The system is going to use an active tag operating on 303 MHz. They states that using this frequency, it operates well outside the frequencies used by other medical and scientific telemetry systrems at hopitals. They will by doing this avoid interference with existing eqiupment. In this case the RFID reader are all equipped with wireless 802.11b capabilities to relay data to the hospitals' inventory management system. (Note: According to [43], this frequency cannot be used).

7.16 Use of Java powered iButton from Dallas Semiconductors

One source of future potensial for RFID applications are the use of RFID in conjunction with Internet connectivity and Internet applications. The java powered iButton are running a Java Virtual Machine [65]. This RFID transponder are a tag for the future. It can actually run JAVA applets. It has a 1024-bit Math accellerator and performs public key cryptograhy is less than a second. It is especially designed to be used for Public Key Infrastructure (PKI) applications. The latest versjon can store up to 30 private keys and X.509 digital certificates. One reason for this to be a promising application for the future especially in Norway is that the Government are currently launching an iniative to promote the start of using PKI in the public arena as well as in business areas. According to the National Strategy for IT-security [66] the target for PKI is to have several providers of digial certificates by the end of 2005.
By using the iButton you can store digital certificates for your online bank services and thereby be able to authenticate the web service. By checking that the published digial certificate at the web site with the one you have stored in your iButton and verifying that they are the same you have authenticated with your online bank. You have actually established that the service offfered on the web, is the service it claims to be. You can also digitally sign an encrypt your E-mail. You can also use it for logon for for desktop computer. Since no agreed standard for storing digial certificated to be used for PKI has been selected it is open for all different vendors to offer a good solution. One solution could also be to use smartcards(simkort) but then you have to have your phone or cards with you. With iButton you can keep the RFID transponder in a wristwatch, ring, key-ring etc. The flexibility are amazing. Why use RFID tag for storing this information and not just store it on your PC? Because if you are careless or unlucky hackers can get access to you computer, either by remote login or using a spyware program which searches your computer for passwords and keys and sends them to the attackers machine. Simply storing your secret keys on computer is not secure enough.
The RFID reader would be a simple cheap device connected to either serial, paralell or USB port on a PC or PDA for that matter. The iButton offers the use of SHA-1, DES, 3-DES and RSA cryptographic algorithms. The storage capcity are up to 134kByte of memory. The iButton is certifiec by the US Government meeting the Federal Information Processing Standards Publication 140-1 Security Requirements for Cryptographic Modules. (FIPS 140-1) [67].

7.17 Statements on future use of RFID Applications

United States Department of Defence

The US DoD [69] announced in October 2003 [68] that by January 2005 all suppliers had to attach RFID tags to virtually all products delievered to the military. The mandate specifies that the tags must be attatched to the lowest possible level of product. The proposed policy requires passive tags to be used but it is expected that the final release of the RFID policy and implementation stragegy will be announced in July 2004.

US department of defence planning widespread use of RFID. DoD is about to to mark anything from missiles to medical supplies with RFID allowing these items to be continously teracked. The bottom line seems to be a policy where any supplier delivering goods to the armed forces will have to RFID mark their products. This is due to the trend where forces are required to be deployable in a minimum of time and where logstics will play a major role thus the less manual routines the better hence a transformation towards a "high tech force". By the use of RFID each single part delivered can be tracked and logged along the way from "vendor to foxhole" making sure that the origin of the product is what is said on the packaging and that equipment returned for reapir really is repaired when returned. A major factor is also the need to get control of the inventory in various containers and storehouses in the campaign area. The idea is to use active tags on larger objects as containers and planes whilst passive tags will be used on pallets and cases. This work will be made far easier as the industry in general adopts the RFID technology at the expense of the outdated barcode. This process will most likely be accellerated by the ongoing work of global standardisation. The frequency used for the pilot finished early in 2004 was 2,45GHz. Pallets was equipped with tags and a reader was mounted on a forklift used to move the pallets within the supplyarea. A local computer keeping track of the inventory was automatically updated as containers passed arriving the depot area. Another dimension to the concept is the logistics of food where time matters versus an expiration date fixed by the producer. Tags with onboard temperature sensors allow the temperature to be measured continously from vendor during transport until the shipment arrives at the camp.

Microsoft establishing RFID alliance on their own

By this move MS are following other major actors within the computer industry in their increased focus on RFID technology. Among these are Oracle and IBM. An own council named "Microsoft RFID council" has been founded as a first step in an increased engagement to launch a RFID policy based on the MS platform. The main task of the council will be to identify the requirements for the emerging platform.The first meeting is to be hold in April 2004. Another decision taken by MS is to be a member of EPC global fronting the international engagement in forming RFID standards on a international basis. This implies that Microsoft software will be capeable of handeling huge amount of data delivered by RFID readers representing end user systems. This also includes the CE operating system. By doing this MS stakes its vlaim in the boosting marked for RFID applications. Three phases are identified where the first implies how to comply with

RFID mandates, the second deals with getting enterprisesd into business by RFID, and the third stage adresses the cooperation between business partners.

Wal-Mart

Wal-Mart has also announced [70] in 2003 that its 100 largest suppliers must have to identify cases and pallets with RFID tags by January 2005.

8. Framework for RFID Application evaluation

In the previous chapters we have aimed to present an overview of the technology. Furthermore we have presented samples of the classical RFID applications by which many are in active use as we speek. Next we delved into the extensive reasearch beeing done in the search for new and promising RFID applications for future use. It has been said that the ultimate RFID killer application remains to be found. Still the opportunities to achieve this goal has never been better as a result of larger memory, sensors, processing capacity and longer range. In order to discuss what applications that might stand better chances than others for a commercial breakthrough, we will establish a framework of factors that will have to be considered before an application is launched. Obvious examples are operating frequency and range. Additional matters of interest would be the regulation of frequencies in a particular country or region. Another question is whether well established standards are crucial for the application to be launched as the case might be for a multinational enterprise.

To be able to evaluate and thereby provide advise on what new RFID applications that could have good prosepcts to successful, we need certain evaluation criteria. We need a framework with certain parameters that the properties of the new RFID applications can be evaluated against. Based on our findings when studying the RFID technology and its properties, ongoing RFID standardisation, Government regulation of the frequencies used by RFID applications, security requirements, ethics & privacy considerations, properties of existing RFID applications and properties of RFID applications in recent research and development, we will establish parameters for an Evaluation Framework. Suitable parameters would be such as:

- Technical selection criteria for the RFID components to be evaluated for a RFID application.
- Requirement for standardisation.
- Are frequencies within regulated frequency bands – regulatory issues.
- Requirments for security features.
- The application’s impact on consumer privacy and ethical considrations.
- External factors as the price of tags and the number and value of the items to be tagged.

8.1 Considering the technology

The technology has matured considerably during the recent years. Development on integrated circuits has boosted reasearch on new RFID tags and readers. Features such as using microprosessors and more memory opens up potential new areas for new applications. Also new and small tags with temperature sensors are now a reality. These can automatically log temperature to be continously stored on the tag or to be transmitted to a database after beeing interrogated by an RFID reader. The tags can be one of two millions linked together by the internet. We end up with a list of parameters check for when evalutating the potential implementation of an RFID application. We must carefully consider the applications need for advanced and expensive features versus the ability to carry out a solution based on less exclusive but more reasonable and passive technology.

Active or passive tags:
Active tags provides longer ranges and can also power memory and processors while passive tags are powered by the received power only. This leaves the passive tag with an almost infinite lifetime while active tags needs battery replacements on a regular basis. The type of tag also reflects the value of the tagged item.

Frequency of operation

Frequencies of interest are in the range 100 KHz to 5.8GHz.. Up to 13.56 MHz the information is transferred by inductive coupling. In the GHz domain however transmission is taking place due to true electromagnetic radiation by propagating radio waves. At these frequencies the damping effect is considerable compared to lower bands and their ability to penetrate obstructions along the way of propagation. These effects can be exploited in a number of ways and applications.

Range of transmission

Even the transmission range increases with higher frequencies while the lower bands are used in security applications as admission control and security applications. This effect can be further influenced by the use of an additional onboard battery in order to achieve transmission over longer distances.

Datarate

Low frequency transmission means a low datarate and high frequency in the GHz range means high datarate. This reflects the actual application as car tolling only leaves the tag available for reading in a very limited amount of time. If the amount of data is considerable this requires the transmission to be done over even higher frequencies. In contrast reading a tag with only the manufactorer serial number in an aninal tracking application could be done by very low frequencies.

Risk of interference

Representing RF signals there will always be a risk of interference between RFID equipment and other electronics beeing situated in the area of interest. Typically examples of vulnerable areas are hospitals, factories and airports and implementation of RFID systems in these environmets therefore requires extra consideration to be taken. For the lower band operating ranges are strictly limited thus reducing the risk of interference to a minimum. Also applications making use of medium band frequencies offers good characteristics as far as interference is concerned. Finally the problem is more widespread for the upper frequency bands transmitting over longer ranges thus increasing the risk of potential problems.

Table 11 - Technology framework

Technology factors	Frequency of operation	Range of transmission	Data rate	Risk of interference
Passive tags	Low band <100 KHz 100-500 KHz	Short range	Low	Low
Passive or active tags	Medium band 10-15 MHz 860-930MHz	Medium range	Medium	Low to medium
Active tags	High band 2,4-5,8 GHz	Longer range	High	Higher risk for interference

8.2 The impact of standardisation

We would like to consider the standardisation of RFID. How important is standardisation and will standards help promoting new RFID applications? Progress on the ongoing standardisation work is slow. New concortiums are being created in addition to the existing ones. The fact that the big organisations are hugely involved in the RFID standardisation work is reassuring. EAN International, which was leading the work of evolving barcodes in Europe, is one of the main players in EPCglobal.. Also ISO and ETSI are major contributers on the field of developing standards for RFID. To be able to throw light on this, we need to look upon what standards that exist today and clarify whether the existing RFID applications are based on these standards or not. Furthermore, does it exist RFID applications that do not rely on standards? Having investigated standardisation within RFID we see that ISO has developed several standards for this purpose. The areas where standards are established are as noted before, within agricultural electronics where it has been applied to animal identificatison, cards and personal identification, automatic identification and data capture techniques, freight containers, identification and communication and intelligent transport systems. Many of the existing RFID applications are also within these areas. It is therefore quite clear that standardisation has been at least one of the driving forces for developing new RFID applications. We also see that within certain areas, the standardisation work has not had that much importance. One area is for electronic article surveilance (EAS) systems. We have not been able to document any standardisation results for this application, but the need for standards have also been limited. The EAS systems are only expected to work within one shop or chain of shops. One system can be designed by one manufacturer for implementation in one chain of shops while another is installing equipment from a second manufacturer. Beeing members of different chains they do not have the need for interoperability. This shows us that if the RFID applications are local applications only without need for interoperability, the importance of standards are much less. When considering the importance of standardisation one also need to look at the need for the application to be interoperable with other areas. Standards also promote the spread of an application to different countries. If something is standardised, two different manufactures can use the same standards and tag products. The wholesalers can then use the products from both manufacturers in for example their inventory systems. EPCglobal is one of the leading parts in the work for RFID standisation for supply chain management. The fact that multinational companies like Hewlett Packard and Microsoft have joined the EPCglobal consortium is an indication showing us that RFID is a technology that could have huge potential for the future and that the above mentioned companies have realised this. We end up with the table below to measure the importance of standardisation.

Table 12 - Standardisation framework

<table>
<tr><td rowspan="3">Standardisation</td><td colspan="3">Requirement for interoperability</td><td colspan="3">Requirement for global application</td></tr>
<tr><td>Low</td><td>Medium</td><td>High</td><td>Low (Local)</td><td>Medium (Within country)</td><td>High (Global)</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

8.3 The importance of Frequency Regulation

One other parameter to consider would be the regulation of the frequency spectrum. What impact has the regulating of the spectrum had on development of new RFID applications. We have documented that the frequency band from 9KHz to 400 GHz are regulated. This tells us that you must consider regulation for any RFID application.. Having seen that the ITU are publishing the Table of frequency allocations and that both Europe and USA are coordinating their regulating activities within ITU. FCC and NTIA are coordiating their regulating at the ITU conferances. We have documentet that the European countries are coordinating their regulating activities with CEPT and a lot of the work that regulates RFID applications are conducted by the Short Range Devices Maintenance Group. Also we have seen that the European Union and the European commission are coordinating their activities within CEPT and establishing working groups within EU to cooperate with CEPT. The REC ERC 70-03 which is maintained by the SRDMG provides the details of frequency bands and power limits the different RFID applications must comply with. These facts are providing us with the information that if you want to investigate a new frequency band for RFID applictions you must check with the ERC 70-03 and the ITU table of frequency allocations. Those documents provides all the information needed to establish what frequency bands that can be used and what power restrictions exists. We have also documented that certain frequency bands have been allocated specifically for RFID applications. The referred documents will also tell what frequency bands that can be used anywhere in the world, or if there are restrictions in certain countries. To summarise this we need to check with this table and thereby give advise if a new RFID application could have prospects of beeing widely used. If the frequency band used and power output falls within the regulations, you would have an application that could have potensial to become global. You can also look at the existing RFID applications to see that this is important. All current frequency bands used by RFID applications today falls within regulated bands. Therefore this parameter, regulation of frequency bands and power, is an important parameter to consider when giving advise on future propects of RFID applications. When looking at more generic applications and not spesific, as we are going to do, the actual emitted power would not necessary be known. In our framework we will therefore not consider emitted power as a parameter when evaluating the new RFID applications. When considering regulation we end up with the table below.

Table 13 - Regulation framework

Frequency band regulation	Are used frequency band assigned to RFID applications		Compliance with power limits	
	Yes	No	Yes	No

8.4 Requirement for Security Features

Another factor to consider is the requirement for security. By looking at the documented security requirements in some RFID applications you see that security has vital importance for whether the RFID applications could be used or not. For other types of RFID applications the security has no impact at all for the success of the application. Therefore it would be in the nature of RFID applications to decide the importance of security features. During the last 10 years there has been development of more mature RFID applications within the fields of Toll Road Collection and Access control. This can be viewed in conjunction with the development on the memory capasity on the RFID tags and the tendency to implement microprocessors on the tags as well. This would be an enabler in innovative new RFID applications requireing security features. An example of this is the Java powered iButton from Dallas Semiconductors which has an 1024-bit Math Accellerator being able to perform encryption and decryption using SHA-1, DES, 3-DES and RSA cryptographic algorithms. Since the security requirement for these RFID applictions now can be met in a much better way, it could be one of the reasons for the more widespread use of security features in new RFID applications. As the applications grow more reliable more people trust the technology and more companies would be more receptive and this would have an impact on the number of companies implementing new RFID applications. We have documented that security features can easily be provided, but this requires tags with a certain memory capasity and processing capabilities. This often requires an active tag with battery installed. The cost of these tags are much higher than for passive tags. The need for security features would therefore be difficult to implement if the number of tags required is very high. For our security framework we end up with the table below.

Table 14 - Security framework

Security	Requirement for security features				Number of tags required		
	None	Low	Medium	High	Low	Medium	High

8.5 Considering Ethics and Privacy

Yet another factor that has been clear to us while working with this master thesis is the ethics and privacy considerations one must have in mind when considering implementation of a new RIFD application. Currently only some of the existing RFID appliction has impact on consumer privacy. The Norwegian Data Inspectorate has expressed concern for the protection on privacy using the new Toll Road RFID system in Norway. Even though the company has got permission to use RFID technology, despite that consumer are not informed whether the informtion of their movements are beeing deleted or not. We have also documented that Benneton had to postpone their plans to implent RFID in their clothes due to a strong public opinion. We have seed that MIT conducted an RFID privacy workshop to discuss areas of concern. Furthermore we have documented proposals from reasearch institutions on how to overcome the obstacles when dealing with new RFID applications and protection of privacy. The fact that it has been discussed at these research organisations and that the authorities for enforcing legislation for protection of privacy are very clear of the potensial violations of privacy when using RFID applications, emphasise the fact that this is a very important parameter to take into consideration, when giving advise on prospects for future RFID applications. When implenting an RFID application you must ensure that the legislation in the countries concerned is not violated. For certain activities when you register consumer activities you must apply for a permit to actually do so, before the application can be launched.

To conclude this section the discussion show that we have documented the importance of takeing ethics and privacy into consideration when working on research and development on new RFID applications. Failure to consider this parameter could result in total failure for an RFID applications that you have put much time and investment into. Our framwork for considering ethics and privacy is detailed in the table below.

Table 15 - Ethics and Privacy framework

Considering Ethics and Privacy	Could the use of the applications be considered non-ethical		Are people going to wear products with RFID tags		Could people's whereabouts be tracked		Compliance with privacy legislation	
	Yes	No	Yes	No	Yes	No	Yes	No

8.6 Other external factors

In addition to the already discussed factors to consdider there are others that also would have impact on the deployment of new RFID applications. As discussed in chapter 8.1 quite much has happened on the development on the technology. This has also had impact on the price of tags and the mass production techniques. As shown in chapter 2.12 the cost of tags has dropped very much the recent years and when they are manufactured in large quantities the costs are also reduced. The cost issue is also important when you consider the number of items to be tagged. If only 100 items are going to be tagged, the cost of tags are not that important in relation to when 100 billion items are going to tagged. Obviously in this case the the price is of vital importance. When discussing the cost of tags one must also consider cost of the tagged item. It would not be worth while to tag a 1 dollar with a 2 dollar tag. Therefore this factor is of vital importance to the adoption of RFID technology and must obviously be taken into consideration.

Table 16 - Other external factors framework

Considering external factors	Cost of tag		Value of item to be tagged		Number of items to be tagged	
	Low	High	Low	High	Low	High

9. Evaluation of new RFID applications

We have now created a framework for evalutating new RFID applications. Based on our findings we will evaluate and make comments on the future prospects for 5 different new RFID applications that we find interesting based on the documented research and development projects in chapter 7. We will evaluate, based on the developed framework, whether these could have good prospects for future use. We will only evaluate these 5 because it would be a task far too comprehensive to evaluate all the different new RFID applications identified in reasearch and development projects.

9.1 Supply chain management comprising Manufacturing, Wholesale dealer and Retail

The total concept are detailed in this figure, made by Auto-ID,now called EPCglobal.

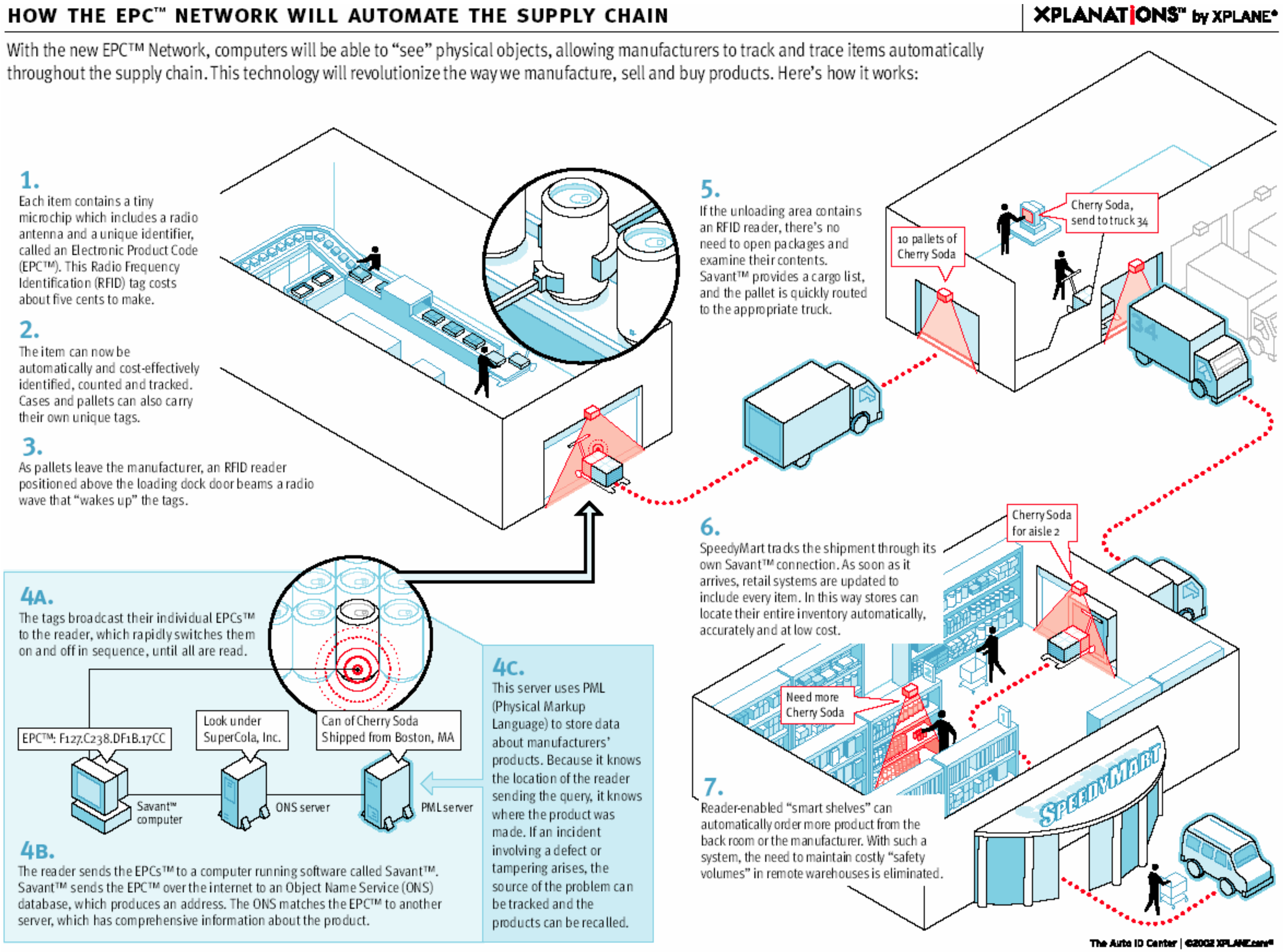

Figure 15 - EPCglobal supply chain management system

During manufacturing each item is equipped with a RFID tag for unique identification. This will probably be implemented in due time, by each manufacturer, as the technology is adopted. All items will be registered by a RFID reader as the pallet leaves the factory. After shipping from the factory the pallet arrives at the wholesale dealer. An example would be a concept comprising electronic gates to register the pallets of goods as they arrive or leave the storage building, updating the stock automatically. Finally the order from the retailer is handeled at the wholesale dealer and goods is transported to the warehouse loading ramp. An application provides updated information about stock or inventory. Goods are added to the inventory system as shipments arrive at the loading ramp. As consumers remove articles from she shelves, the inventory system automatically places orders to update the stock.

There will be numerous other possibilities for utilising RFID technology for inventory purposes. This concept could be customised to almost any enterprise.

Technology

Table 17 - Using technology framework – Supply chain management

Technology factors	Frequency of operation	Range of transmission	Data rate	Risk of interference
Passive tags	Low band <100 KHz 100-500 KHz	Short range	Low	Low
Passive or active tags	Medium band 10-15 MHz 860-930MHz	Medium range	Medium	Low to medium
Active tags	High band 2,4-5,8 GHz	Longer range	High	Higher risk for interference

The draft specifications details HF and UHF tags. The UHF tags would have a range between 2-10 meters and the HF tags much less. As far as type of tag is concerned this application area is most often associated with passive tags. This is due to the fact that the transport of pallets or packaging is controlled until moved out of the storeroom for transport. Thus readers can be installed in strategic places allowing the items to pass close by for registration. Transmission over a short distance will most likely be sufficient for this kind of application. Given that the information stored on the tags is limited to a unique number, it will not be neccessary with a medium or high datarate. Obviously the amount of information stored will vary, but compared to barcodes a few bytes should do to to keep track of serial number, price and other relevant information. Interference should not be a problem as this is a closed area with little risk of disturbance from other systems. Interference could be a potential problem when integrating tags in metal objects. The nature of interference would be bit errors when read and write operations.

Standardisation

Table 18 - Using standardisation framework - Supply chain management

Standardisation	Requirement for interoperability			Requirement for global application		
	Low	Medium	High	Low (Local)	Medium (Within country)	High (Global)

EPCglobal has made proposed standards for tags in both the HF and UHF band. The tag specifications specifies a 64bit and a 96 bit tag. These specifications have the potential to become global since the concortium consist of participant from the whole world. The interoperability requirement for this system would potentially be medium to high and the global requirements would also be medium to high.
The size of the enterprise could have bearing on the need for both interoperability and global applications. The number of suppliers to an enterprise will also have bearing on the implementation of an RFID application, since all different products from the different suppliers need to be tagged with same type of tag. Given a major multinational enterprise the cost of implementing RFID solutions on an early stage could be a hazardous venture, if one were to rely on different vendors and standards from one country to another. A worst case scenario would be if a few years later the work of standardisation changes direction or one could risk to depend on a few vendors to deliver the equipment. On the other side interoperability among vendors and suppliers worlwide would guarantee access to equvivalent equipment no matter in which country or part of the world the business is sited. Most likely this will have positive influence on the prices as well. In times where neither the ongoing work of standardisation nor the technology itself has setteled, many will choose to stay put until these matters are sorted out.
A small national enterprise comprising a small number of units on the other hand could implement an application based on early components at an early stage of the standardisation work and do so to a limited cost. This will provide valuable experience in putting the technology to use and thereby get a lead on its competitors before the expected main stream of adopters joining in when the odds are perceived better for implementation.

Regulation

Table 19 - Using regulation framework - Supply chain management

Frequency band regulation	Are used frequency band assigned to RFID applications		Compliance with power limits	
	Yes	No	Yes	No

This criteria is cruical to any application implementation within a given country or region. The specifications details using regulated frequency bands of 13.56MHz and 860-

930MHz. A future specification are planned in the UHF band with better read range. In this case used frequencies are not specifically just assigned to RFID, but to Short Range Devices. It will be far more demanding and expensive to sort out this matters if enterprises are to be established in a number of countries and even across continents. Again this aspect can be easier dealt with given that the enterprise subdivisions are located to one or even a few countries. We do not have any information about power levels but expect that this will be within regulated limits.

Security

Table 20 - Using security framework – Supply chain management

Security	Requirement for security features				Number of tags required		
	None	Low	Medium	High	Low	Medium	High

Manufacturing and wholesale dealer facilities are often limited and enclosed areas not available to unauthorised personell thus reducing the risk of eavesdropping the communication between tags and readers. Put in another way mechanisms as encryption and autenthication would most likely not be required, reducing the demands on datarates and thereby beeing able to operate on lower frequency bands. Therefore the security requirements for this potential application would be low to medium. At the retailer however this is a matter of increasing interest as the customer, now introduced into the chain, might be challenged to tamper with the established systems in order to gain personal profit or benefits. As a consequence of this proper measures should be taken to prevent unauthorised from writing to the tags and thereby altering the original content.

Ethics and Privacy

Table 21 - Using security framework - Supply chain management

Considering Ethics and Privacy	Could the use of the applications be considered non-ethical		Are people going to wear products with RFID tags		Could people's whereabouts be tracked		Compliance with privacy legislation	
	Yes	No	Yes	No	Yes	No	Yes	No

In the manufacturing process the potential problems of ethics and privacy is considerably reduced as the entire production is concentrated within a limited area. Another fact is that customers and buyers are not present at this stage eliminating the potential for exploitation of information originating from tagged products bought by customers at

retailers. It seems hard to find any critical aspects regarding ethics and privacy at this level of the supply chain.
For the last stage in the supply chain, at the retailer, the tags would most likely be used for products that people are going to wear. This could be a potential problem. This is an area of great controversy as the good intentions of the application owner might be abused by outsiders. A tagged product that is taken down from the shelf and paid for by the till should have its tag removed in the same operation. If this is not the case the customer could unawarely be a victim of producers making statistics over their own products by scanning your shoppingbag later on. If the item of interest can be associated with your own person then even your whereabouts can be tracked as the case might be with airplane tickets, mobile phones and so on. In this case it can be considered as non-ethical. This issue has been thought of and in the specifications there have been detailed a possibility for a kill command. This command would set the tag in a state where it is not responding to a RFID reader. The specifications do not detail anything regarding compliance with privacy legislation but when implementing such a system these issues must be clarified before the application can be launched.

External factors

Table 22 - Using external factors framework - Supply chain management

Considering external factors	Cost of tag		Value of item to be tagged		Number of items to be tagged	
	Low	High	Low	High	Low	High

It lies in the nature of supply chain management that these three factors will have a major influence on the totalt cost of implementing RFID technology. Articles produced by maufacturers will as a rule of thumb not be equipped with active tags as readers can easily be placed along the production chain in order to monitor the process continously. In the same way, as far as the cost of the item is concerned, the rule is that the cost of the tag should not exceed the cost of the item to be tagged. As a result of this tagging of most items in the manufacturer – wholesale – retail chain could be done by use of reasonable passive tags. Examples of more costly items to be equipped with active and thus more expensive tags would be cars, boats and motorcycles. The value of each item would justify the price of the tags required.

As with the manufacturer scenario the wholesaler is another case featuring a rather large number of items originating from av number of manufacturers. According to this the number of tagged items in transit would be rather large. Another similarity is that the items in question are easily tracked at the loading ramps reducing the need for readers to a limited number of places. As a result of this, the solution could be realised by passive technology. In general the cost of the items is not considered to be particularly high reflecting the use of passive tags. In the retail link of the chain there are several similarities to the manufacturer and wholesale link in the supply chain. The products can easily be registered at choke points as they enter and leave the warehouse through the loadingramp and the till respectively. By placing readers at these points the flow of articles can be logged by passive technology. Originating from the manufacturer via the wholsaler the number of tagged items in circulation could be considerable.

9.2 Asset tracking of important or valuable objects

By providing valuable assets with a tag, you will be able to track the location at any time.

Technology

Table 23 - Using technology framework - Asset tracking

Technology factors	Frequency of operation	Range of transmission	Data rate	Risk of interference
Passive tags	Low band <100 KHz 100-500 KHz	Short range	Low	Low
Passive or active tags	Medium band 10-15 MHz 860-930MHz	Medium range	Medium	Low to medium
Active tags	High band 2,4-5,8 GHz	Longer range	High	Higher risk for intererence

Asset tracking, as the name implies, enables an item to be localised by its associated tag. Depending on the actual application the tracking range could vary widely and most likely up to about 30 meters or so. This requires longer ranges of operation than can be achieved by the use of passive transponders. Given this fact we notice that the appropriate range of frequency is within the GHz area thus enabeling higher datarates but also raising the costs attended with the implementation. The value of the items to be tracked should be considered carefully in relation to the cost of the active tag. The surroundings for the area where the application is to be used should be chosen with care as interference with existing electronic environments might take place. Vulnerable areas could be airports, hospitals and factories.

Standardisation

Table 24 - Using standardisation framework - Asset tracking

Standardisation	Requirement for ineroperability			Requirement for global application		
	Low	Medium	High	Low (Local)	Medium (Within country)	High (Global)

Once again the importance of established standards plays an important role as one must determine the extent of the solution. In order to cover sites in several parts of a country or even across several countries a connecting network is required and thus the need for standardisation. However this should not affect stand-alone solutions that could exist happily in one country even if it could not be realized elsewhere. This will also have an effect on the interoperability issue as investments will be limited.

Regulation

Table 25 - Using regulation framework - Asset tracking

Frequency band regulation	Are used frequency band assigned to RFID applications		Compliance with power limits	
	Yes	No	Yes	No

As with all RFID applications the regulation issue is very important to comply with, but if you have compliance, regulation would not be an obstacle. With asset tracking it is also important that the equipment comply with regulation both on using assigned frequency band and power restrictions. Since we are not evaluating a specific application we would not know what frequencies are used but we have suggested that applications should use the GHz bands. Here you have 2.45GHz and 5.8GHz ISM bands for available for RFID.

Security

Table 26 - Using security framework - Asset tracking

Security	Requirement for security features				Number of tags required		
	None	Low	Medium	High	Low	Medium	High

In the nature of this application lies the fact that in order to defend the cost of the active tag the tagged item should be of a certain value. This should be reflected in the mechanisms applied to secure the communication channel so that the risk of tampering and fraud can be limited to a minimum. Items of interest could be tools, surgical instruments or materials at a building site. The number of tags is expected to be relatively low.

Ethics and Privacy

Table 27 - Using ethics and privacy framework - Asset tracking

Considering Ethics and Privacy	Could the use of the applications be considered non-ethical		Are people going to wear products with RFID tags		Could people's whereabouts be tracked		Compliance with privacy legislation	
	Yes	No	Yes	No	Yes	No	Yes	No

This matter is totally dependent on the nature of the object. A boat or a car could easily be tracked at certain points of interest and thus tracking the movements of its passengers as well. This would require a network over which the information could be excahnged. Also the tracking of a tool could, to a certain extent, reveal information about the person using it. Therefore this application could potentially be considered to be non-ethical. Compliance with privacy legislation could, and could also not be the case.

External factors

Table 28 - Using external factors framework - Asset tracking

Considering external factors	Cost of tag		Value of item to be tagged		Number of items to be tagged	
	Low	High	Low	High	Low	High

This application enables objects to be tracked in order to pinpoint their location at any time. This implies tracking over a certain range requirering active and more expensive tags. This fact is reflected in the value of the tagged item as this might be objects of high value or importance such as surgical instruments or equipment on a construction site. Due to the cost of the tags, the number of items to be tagged will typically not be very large.

9.3 New services featuring mobile phone with integrated RFID reader

One possible application using this concept would be to mount RFID tags on key objects along a watchmans route. On his route he could indicate his position by the use of his mobile phone thus updating the headquarters of his whereabouts.

Technology

Table 29 - Using technology framework - Mobile phone with integrated RFID reader

Technology factors	Frequency of operation	Range of transmission	Data rate	Risk of interference
Passive tags	Low band <100 KHz 100-500 KHz	Short range	Low	Low
Passive or active tags	Medium band 10-15 MHz 860-930MHz	Medium range	Medium	Low to medium
Active tags	High band 2,4-5,8 GHz	Longer range	High	Higher risk for intererence

A reasearch project featuring this concept allows watchmen to mark their position at an object by touching a point (tag) dedicated for this purpose identifying their position. The only information needed is the unique code of the tag thus the application can be realized by the use of a passive system featuring a low datarate. This will reduce investments yet the spesialized mobile phone will add costs to the solution. This might be worth while as the application might give the headquarters an early warning of potential assaults threatening both lives and values. This specific phone uses the frequency band of 13.56MHz and operate at short ranges. It would be a very low risk of interference.

Standardisation

Table 30 - Using standardisation framework - Mobile phone with integrated RFID reader

Standardisation	Requirement for interoperability			Requirement for global application		
	Low	Medium	High	Low (Local)	Medium (Within country)	High (Global)

This specific system on the Nokia phone uses the ISO14443 standard for inductive applictions. The fact that this system uses a standardisaed interface improves the interoperability possibilities for this application. Also that this is an global standardard produced by ISO shows that it could be used globally. Saying this, how the application uses the information collected by the RFID reader, is not subject for standardisation. We would expect the requirement for both interoprability and globaness to be medium.

Regulation

Table 31 - Using regulation framework - Mobile phone with integrated RFID reader

Frequency band regulation	Are used frequency band assigned to RFID applications		Compliance with power limits	
	Yes	No	Yes	No

For this specific RFID application the ISM frequency 13.56MHz is going to be used. We have no information about field strength for the reader in the phone, but we expect the operation to be within regulated limits. This means that there would be no problem regarding regualtion using this appliction globally.

Security

Table 32 - Using security framework - Mobile phone with integrated RFID reader

Security	Requirement for security features				Number of tags required		
	None	Low	Medium	High	Low	Medium	High

It would be of vital importance to the watchmen, and and the company, as such that this localisation info is passed on to the headquarters with no possibility for outsiders to pose as watchmen or preventing an confirmation to be sent. Enhanced security could be achieved by duplicating the message by utilising both the mobile channel and an alternative solution by the fixed telephone network originating from the tag. It is expected that the number of tags for this type of RFID application to be low.

Ethics and Privacy

Table 33 - Using ethics and privacy framework - Mobile phone with integrated RFID reader

Considering Ethics and Privacy	Could the use of the applications be considered non-ethical		Are people going to wear products with RFID tags		Could people's whereabouts be tracked		Compliance with privacy legislation	
	Yes	No	Yes	No	Yes	No	Yes	No

This would definately be a suitable case for discussing the issue of ethics and privacy related to the RFID technology and its applications. The monitoring is limited to the fixed points on the watcmans route as he is only carrying the reader of the system. Even if this system will roughly track the watchmans movements, you could say that this is in the benefit of the watchman. His personal security would be very much improved by this RFID application. Therefore we would not categorise this application to be non-ethical. If this application would comply with privacy legislation would be difficult to determine. It depend on how the information gathered is used.

External factors

Table 34 - Using external factors framework - Mobile phone with integrated RFID reader

Considering external factors	Cost of tag		Value of item to be tagged		Number of items to be tagged	
	Low	High	Low	High	Low	High
			N/A			

In this case the cost of the tag will be modest as passive technology will be sufficient for marking the object of interest. The value of the item is not considered to be relevant for this particular application as this might be buildings or other infrastructure marking a position. The number of "checkpoints" or items to be tagged is expected to be rather limited depending on the actual application. An example would be watchmen confirming their position at objects along their route. An additional cost however would be the number of RFID equipped mobile phones required for this particular applications.

9.4 New services featuring RFID tags with integrated temperature sensors logging ambient temperature

This would ensure food quality during transport from supplier to retailer. This could be one of several possible implementations.

Technology

Table 35 - Using technology framework - RFID tags with temperature sensors

Technology factors	Frequency of operation	Range of transmission	Data rate	Risk of interference
Passive tags	Low band <100 KHz 100-500 KHz	Short range	Low	Low
Passive or active tags	Medium band 10-15 MHz 860-930MHz	Medium range	Medium	Low to medium
Active tags	High band 2,4-5,8 GHz	Longer range	High	Higher risk for intererence

This application is another one featuring active tas as an integrated temperature module is required to continously log the temperature of the surroundings. This means that a certain amount of memory must be present in order to store the temperatures logged for later use and presentation. How much memory that will be needed will depend on the logging interval thus determining the lifetime of the tag as well before batteries must be replaced. Still the datarate could be rather low only representing the current temperature say two times a day. As active tags in general are more expensive than passive tags, the cost will be rather high compared to regular passive tags. This system would eventually feature long reading range making the application rather flexible as far as the arrangement of readers are concerned. The potential risk for interference would normally be low to medium.

Standardisation

Table 36 - Using standardisation framework - RFID tags with temperature sensors

Standardisation	Requirement for interoperability			Requirement for global application		
	Low	Medium	High	Low (Local)	Medium (Within country)	High (Global)

Implementing an application like this will most likely be a bit more costly than an application featuring passive tags. The tags are expensive yet the number of items to be tagged could be considerable representing major investing costs. As a result of this the matter of standardisation becomes more important as a worldwide marked would yield larger prospects of return on investments. That is after an initial period of developing and testing. In the same way the idea of a global marked emphasizes the importance of interoperability among equipment vendors. How to use these type of tags would be a subject for future standardisation.

Regulation

Table 37 - Using regulation framework - RFID tags with temperature sensors

Frequency band regulation	Are used frequency band assigned to RFID applications		Compliance with power limits	
	Yes	No	Yes	No

Also for this case, we are not looking at one specific application and would therefore not know what frequency band that would be used or if the application would be within regulated limits. As stated in the discussion on the technology typically there would be used active tags with battery power because of processing need. This would not necessary mean that the read range would be long but low to medium. Expected frequency bands for these applications would therefore be expected to be in the VHF band. There are frequencies available for RFID applications in the VHF band. The devlopers of new applications must also make sure they comply with power restrictions for selected frequency band.

Security

Table 38 - Using security framework - RFID tags with temperature sensors

Security	Requirement for security features				Number of tags required		
	None	Low	Medium	High	Low	Medium	High

If used for surveilance of food articles and the temperatures they are exposed to from manufactorer to the end consumer, security is not likely to play a major role. There should be mechanisms to prevent tampering with the information in the logg, but the requirement for security features would generally be low.

Ethics and Privacy

Table 39 - Using ethics and privacy framework - RFID tags with temperature sensors

Considering Ethics and Privacy	Could the use of the applications be considered non-ethical		Are people going to wear products with RFID tags		Could people's whereabouts be tracked		Compliance with privacy legislation	
	Yes	No	Yes	No	Yes	No	Yes	No

This application could easily be compared to any of the applications describing the three links of the supply chain mentioned earlier. Thus there is a risk of the tag not beeing deactivated at the till resulting in continous logging even outside of the store where it was bought. The chances for the information to be read by others remains without the sensor technology adding any new aspects to this scenario. Therefore when considering these kind of applications, the requirement for having the possibility of forcing the tag into an inavtive state must be considered. When implementing these applications you must comply with privacy legislations. The application would not be considered to be non-ethical.

External factors

Table 40 - Using external factors framework - RFID tags with temperature sensors

Considering external factors	Cost of tag		Value of item to be tagged		Number of items to be tagged	
	Low	High	Low	High	Low	High

Compared to a regular passive tag there will have to be additional functionality as sensors and additional memory on these tags. This will naturally result in more expensive tags. It must also be taken into consideration that when applied for food monitoring, the number of units can be high making the total application quite expensive. The value of items to be tagged is expected to be low. An alternative is to share one tag among a number of units as the case would be on a pallet or in a container.

9.5 Human tracking within controlled environments

These are applications with the purpose of tracking certain categories of personell within their authorised areas. Relevant categories of people would be patients or prisoners or even children in an amusement park allowing them to be easily found and reunioned with their parents. Obviously there would be major privacy issues to address related to these applications.

Technology

Table 41 - Using technology framework - Human tracking

Technology factors	Frequency of operation	Range of transmission	Data rate	Risk of interference
Passive tags	Low band <100 KHz 100-500 KHz	Short range	Low	Low
Passive or active tags	Medium band 10-15 MHz 860-930MHz	Medium range	Medium	Low to medium
Active tags	High band 2,4-5,8 GHz	Longer range	High	Higher risk for intererence

In order to effectively track people, there must be a certain area over which the tracking takes place. This requires the use of active transponders with long range operating at frequencies in the GHz area. This is because you would need a system of RFID readers to cover a specific building or part of a building. When selecting frequency it would be best to use the upper UHF bands, 2.45GHz or 5.8GHz, since these have long range. Given the need for a high level of security, it follows that encryption is required. For reliable identification a standard serial number should be sufficient leaving extra datacapacity for other use. Notice that since line of sight transmission is a characteristic of this frequency range, a considerable number of readers should be taken into account at implementation. By limiting the readers to strategic points as doors and entrances however, the total numbers of readers can be reduced implying lower costs The risks for interferance with other applications would also be higher when using these frequency bands.

Standardisation

Table 42 - Using standardisation framework - Human tracking

Standardisation	Requirement for interoperability			Requirement for global application		
	Low	Medium	High	Low (Local)	Medium (Within country)	High (Global)

At the moment there seem to be a certain activity of research on this type of applications. The requirement for interoperability is therefore estimated to be low. Typically this application should only be functioning within one building and with a selected brand for tag and reader. If the tags and readers were using global standards, you could use any manufacturer, but the requirement for this would be low. You could manage with only one provider of tags and readers. Also the requirement for the applications to be working globally would not be vital, reducing the need for standardised products.

Regulation

Table 43 - Using regulation framework - Human tracking

Frequency band regulation	Are used frequency band assigned to RFID applications		Compliance with power limits	
	Yes	No	Yes	No

As disscussed under technology, we would expect this type of RFID application to use the upper UHF band. This kind of application would also need to consider radio regulation, since any use of the frequency spectrum is requlated. There are bands available for RFID, and therefore it should be possible to be able to use assigned frequencies. It would be recommended for these kind of applications to use frequency bands assigned to RFID or to generic Short Range Devices. Also regarding regulated power, any future new RFID applications in this area, must comply with regulations.

Security

Table 44 - Using security framework - Human tracking

Security	Requirement for security features				Number of tags required		
	None	Low	Medium	High	Low	Medium	High

In this case there are identities associated with the tags and therefore a high level of security is required in order to prevent personal information from beeing exposed to outsiders. This complies with the fact that higher frequency bands are required, enabeling higher data rates. The number og tags associated with this application could vary considerably, but is expected to be low to medium. For improved security the tags could contain only a unique number to be mapped into a personal file by the host computer.

Ethics and Privacy

Table 45 - Using ethics and privacy framework - Human tracking

Considering Ethics and Privacy	Could the use of the applications be considered non-ethical		Are people going to wear products with RFID tags		Could people's whereabouts be tracked		Compliance with privacy legislation	
	Yes	No	Yes	No	Yes	No	Yes	No

The issue of tracking people and their wherabouts, is associated with major controversy when it comes to both ethics and privacy. At the moment, any possible applications featuring tracking of people would be considered higly non-ethical, but a gradual change of attitude is expected when time goes by. Despite the protests, there seems to be a growing understanding for the fact that in certain areas this might provide an acceptable solution. In any case it would be of vital importance to comply with the privacy legislation in the country of implementation. Like in Norway, the Data Inspectorate has stated that tagging of humans will only be allowed in very special cases. Provided careful use and consideration, this could be a way of securing people in an institution by allowing monitoring of their movements within the restricted area of a hospital or a mental institution.

External factors

Table 46 - Using external factors framework - Human tracking

Considering external factors	Cost of tag		Value of item to be tagged		Number of items to be tagged	
	Low	High	Low	High	Low	High
			N/A			

This is another application to make use of active tags in keeping track of the wherabouts of people whose movements are restricted to certain buildings or rooms. A certain range of operation will require active technology to be applied. Also some memory might be required for the storage of personal information. This might as well be handeled by a central database. This would reduce the memory requirements to a unique number to be mapped into a profile, when read by the reader. The value of the tagged item is obviously not relevant for this case. The number of persons beeing tracked by an application like this, is likely to be limited reducing the overall cost of implementation.

10. Conclusion

10.1 Supply chain management

To sum up the discussion of these new RFID applications, one could say that provided global standards and regulated frequencies are to be used, the applications should have good prospects of becoming sucessful. The fact that the standardisation work is not completely finished indicates that it would still be a matter of time, until the solutions are ready to be implemented in a larger scale. As noted in the discussion earlier, introducing a limited implementation would be less vulnerable, as later changes in standardisation only will result in a limited replacement of allready installed equipment. A small scale implementation could therefore be forseen within near future. Doing this in an early phase, will also provide considerable experience from pilot implementations, that will be valuable when considering an global roll out at a later stage. Since the future RFID application are planned using regulated frequency bands, regulation should not be an issue, but they still have to make sure that the regulated power limits are not exceeded. The technology is also mature enough to provide necessary security features for these applications. The privacy issues should not be a problem in manufacturing and the wholesale dealer inventory system. On the other hand, this is a major issue in the retail business. The drawback with the retailer application would be the possible privacy implications of people wearing tagged products. It looks like this has been forseen by the authors of the draft standards when specifying the kill command. As long as the privacy issues are not solved, the kill command should be used at the retailer level before the product leaves the store. By doing this, one would avoid the privacy issues with people wearing live tags that can be interrogated by anyone with a RFID reader. Naturally this information could be used to map consumption patterns or making statistics about consumer habits. When it comes to external factors there is no doubt that the price of the tags must clearly reflect the value of the items to be tagged. In most cases, and within grocery trade in particular, passive technology should be adequate indicating a reasonable solution compared to an application featuring active tags. Obviously the number of potential articles to be tagged, will have bearing for the total cost of deploying RFID technology to manufacturing, wholesale or retailing. The prices obtainable from producers of tags will also reflect the size of the order favouring the larger chains.

10.2 Asset tracking of important or valuable objects

Asset tracking of valuable objects is an application that in our opinion also could be tried for an early implementation. The research projects we have documented clearly show that this is possible to implement due to the factors described in the framework. Despite this, there are developments to be expected on the standardisation arena. Given that these RFID applications only make use of allowed frequency bands and operate within maximum power levels, they could have good chances of beeing sucessful. As also mentioned in the discussion, if the tagged items could be associated with persons, the company implementing the RFID application must make sure that they have the necessary permissions from the proper authorities to actually implement the actual RFID application. Considering external factors and the fact that active tags will be most suited for this application, it follows that there should be a limited number of tags involved in order to guarantee the best prospects for return on investment. Never the less, a limited solution will provide valuable experience until the ongoing work on standardisation has setteled, thus limiting potential loss.

10.3 New services featuring mobile phone with integrated RFID reader

As discussed previously these services should be relatively cheap to implement using low cost passive tags. Since the phone uses an ISO standard for tag and reader, this should have influence on the drive for this application to have the potential to be used globally. Also the fact that it would operate wihin regulated frequency and power limits means that regulation would be no issue for the implementation for new services utilising the RFID reader integrated in the Nokia phone. The discussion shows that there could be potential privacy issues to address when the application gives details about persons movements. According to our framework this would be the only potential obstacle for these new RFID applications, that could be applied for many professions operating from a mobile platform. Again, any research and development project should pay close attention to the privacy issues when investigating new services utilising the Nokia phone's RFID capabilities. As long as the privacy issue is solved, new services using the RFID reader should have good chances for becoming sucessful. The price of a RFID equipped phone versus a regular NOKIA mobile phone and the number of units applied in the solution, should also be a keyvariable for the prospects of return on investment. As far as external factors is concerned, it seems clear that this application comprises a limited number of units. Nokia provides complete "business solutions" or kits including phones and accessories ready for deployment.

10.4 New services featuring RFID tags with integrated temperature sensors logging ambient temperature

Despite the fact that tags with integrated sensors allready exist on the marked, the technology is still a bit immature and costly. Also as far as the issue of standardisation is concerned, clear directions remains to be found. For new applications one could utilise existing standardised tag products, but in order to use the technology to its full potential, more standardisation on this field should be awaited before a full roll out of new applications. Also for these applications to be videly used, they must be implemented using regulated frequency bands for RFID applications or Short Range Devices. The low requirement for security features shows that it currently can be implemented. For these kind of RFID applications the dicussion has shown that the privacy issue concerning tracking of peoples whereabouts, must be solved before a full scale implementation can be launched. These tags falls within the category of active tags thus higher cost per tag must be expected. One major area of use would be for control of food quality from producer to consumer. This implies a large quantity of units reflecting the total cost of deployment. In other words, this might turn out to be an expensive venture especially as long as standards are under evaluation. An alternative would be to limit the monitoring to larger quantities as containers or pallets reducing the costs. However, this solution will not provide surveillance of single products for the consumer making purchases at the retailer.

10.5 Human tracking within controlled environments

For this particular RFID application the discussion has shown that the technology is ready to be launched in a small scale as a pilot project. We have documented that standardisation is not crucial in this case, as development of within this field is in an initial phase. Pilots featuring elements of human tracking has been trailed by considerable controversy and numerous discussions. However, objections are expected to be less persistant over time, as the advantages becomes clearer, featuring improved security for the categories of personell involved. Of equal importance is the fact that this can be achieved by relatively simple means, as the areas to be covered are rather restricted, facilitating simple implementation, regarding both labour and cost. Using the right type of tag, and setting up the readers properly, one should easily be able to cover the desired area of interest. Since interoperability concerns are limited in an early phase, requirement for using standardised products is not that high. The dicussion also stated that the requirement for the application to be global would be low. This is probably the application where the privacy issues could be the major hurdle for new RFID application to be launched. Just thinking about implementing these kind of new RFID applications, without starting with addressing the matters of ethics and privacy, would imply a high risk of failure. In Norway, the first step should be to involve the Data Inspectorate and provide a thorough specification of the application in question. Without their concent, all plans would risk to be abandoned at an early stage. Deployment of pilots should be higly feasible as the restricted areas in question, should be easy to control reducing the number of readers to a minimum. Even though active tags are required the number of objects, should be limited, reducing the overall cost and thereby the risk. This would provide valuable knowledge which could be taken advantage of, during a larger roll out at a later stage.

10.6 Conclusion Summary

Table 47 - Conclusion summary - Standardisation - Regulation - Security - Ethics & Privacy

	Standardisation						*Regulation*				*Security*							*Ethics & Privacy*							
	Interoperability			*Global application*			*Assigned*		*Power limits*		*Security features*				*Number of tags*			*Non-ethical*		*Wearing products*		*Whereabouts*		*Privacy legislation*	
	Low	*Med*	*High*	*Low*	*Med*	*High*	*Yes*	*No*	*Yes*	*No*	*None*	*Low*	*Med*	*High*	*Low*	*Med*	*High*	*Yes*	*No*	*Yes*	*No*	*Yes*	*No*	*Yes*	*No*
Supply chain management																									
Asset tracking																									
Mobile phone with RFID reader																									
Temperature sensors																									
Human tracking																									

Table 48 - Conclusion summary - External factors and Technology

	External factors						Technology				
	Cost of tag		Value of item to be tagged		Number of item to be tagged			Frequency of operation	Range of transmission	Data rate	Risk of interference
	Low	High	Low	High	Low	High					
Supply chain management							Passive tags	Low band	Short	Low	Low
							Passive or active	Medium band	Medium	Medium	Low to medium
							Active	High band	Long	High	Higher
Asset tracking							Passive tags	Low band	Short	Low	Low
							Passive or active	Medium band	Medium	Medium	Low to medium
							Active	High band	Long	High	Higher
Mobile phone with RFID reader			N/A				Passive tags	Low band	Short	Low	Low
							Passive or active	Medium band	Medium	Medium	Low to medium
							Active	High band	Long	High	Higher
Temperature sensors							Passive tags	Low band	Short	Low	Low
							Passive or active	Medium band	Medium	Medium	Low to medium
							Active	High band	Long	High	Higher
Human tracking			N/A				Passive tags	Low band	Short	Low	Low
							Passive or active	Medium band	Medium	Medium	Low to medium
							Active	High band	Long	High	Higher

To summarize the conclusions, we have made two tables, table 47 and 48, where the complete evaluation of the 5 new RFID applications are presented.

When considering standardisation the table shows that for almost all applications we have evaluated, standardisation is an important factor to consider when investigation new RFID applications. Until the applicable standardisation have settleled, it would be risky to launch large scale RFID applications. Small scale implementation would therefore be recommended.

The evaluation has also shown that as long as the new applications comply with assingned frequency bands and power limits, regualtion is not a major issue.

When evaluating the aspects of security we found that all of the current applications required some level of security to be implemented. The conclusion would therefore be that alomost all type of new RFID applications require at least a certain degree of security features.

When evaluating new applications on the basis of the framework for ethics and privacy, we found that this is one of the most important factors to take into consideration, when evaluating new RFID applications. Any application violating the legislation of privacy should expect a high risk of getting its rollout terminated or hindered due to privacy issues.

Furthermore, each of the proposed new RFID applications holds unique properties regarding the external factors. Therefore, when evaluating a new RFID application, there seems to be no clear pattern between the external factors comprising cost of tag, value of item to be tagged and number of items. These factors must therefore be seen in context for each new RFID application.

Finally when evaluating on the basis of technolgy, we see that it is the nature of the new RFID application that drives the choice of technology. Where you only need short ranges and low datarate, you would be best served with passive technology in the medium frequency range. This will again result in lower cost, and the potential for return of investment would be better.

This master thesis has shown that even if RFID has proven to be an exciting and promising technology since its invention, nearly three decades ago, its killer application remains to be found. Even with its obvious advantages over barcodes, it takes more than technology itself to succeed in launching an application to guarantee return on investments. Price per tag is vital and declining, but still not comparable to the barcode, unless ordered in enoromous quantities. Standardisation has been slow, but is expected to move forward in supply chain management, since giants like Microsoft and Hewlet Packard have joined the EPCglobal initiative. ISO is also making progress on RFID standardisation. Ethics and privacy turns out to be a matter of equal, or even higher importance. How these issues are dealt with in the next few years, will determine whether this could be the final breakthrough for RFID. We believe this master thesis holds information that could come useful in the process of implementing new RFID applications. By using our developed framwork, any organisation will get an insight, whether their own new RFID application will have good prospects of becoming successful in the future.

References

[1] Teleca Wireless Solutions(TWS), www.teleca.no

[2] Claus Finkenzeller, RFID Handbook, 2003, Edition 2

[3] International Telecommunication Union, www.itu.org

[4] ISO, International Organisation for Standardisation, http://www.iso.org/iso/en/ISOOnline.frontpage

[5] CEPT, European Conference of Postal Telecommunications Administrations, http://www.cept.org/

[6] ETSI, European Telecommunications Standards Institute, http://www.etsi.org/

[7] EPCglobal, http://www.epcglobalinc.org/

[8] RFID Journal, http://www.rfidjournal.com/

[9] Massachusets institute of Technology (MIT), www.mit.edu

[10] Redprairie, supply chain technology supplier, http://www.redprairie.com/knowledge/PDF_whitepapers/RFID-Just_the_facts.pdf

[11] Mario Chiesa et al, RFID – A week long survey of the technology and its potential, 2002, http://people.interaction-ivrea.it/c.noessel/RFID/RFID_research.pdf

[12] IMLink no 6, La Newsletter de l'Institut international de Management pour la Logistique, March 2004, http://imlwww.epfl.ch/imllink/imllink6/page5.php

[13] RFID Journal, Article, 2004, http://www.rfidjournal.com/article/articleview/748/2/90/

[14] ISO home page, http://www.iso.ch/iso/en/aboutiso/introduction/three, accessed 21 May 2004.

[15] ISO, International harmonized stage codes, http://www.iso.ch/iso/en/widepages/stagetable.html#90, accessed 21 May 2004

[16] ITU-R, ITU Radiocommunication Sector, http://www.itu.int/ITU-R/

[17] ITU-T, ITU Telecommunications Standardisation Sector, http://www.itu.int/ITU-T/

[18] ITU-D, ITU Telecommunication Development Bureau, http://www.itu.int/ITU-D/

[19] ETSI ERM, http://portal.etsi.org/erm/Summary.asp , accessed 24 May 2004

[20] UCC, Uniform Council Code, http://www.uc-council.org/mission.html , accessed 24 May 2004

[21] EAN International, http://www.ean-int.org/ , accessed 24 May 2004

[22] EAN.UCC, http://www.ean-ucc.org/ , accessed 24 May 2004

[23] EPCglobal, http://www.epcglobalinc.org/ , accessed 24 May 2004

[24] EPCglobal, Standards Developments Process, http://www.epcglobalinc.org/standards_technology/040130%20EPCglobal%20SDP%20Spec.pdf, accessed 30 March 2004

[25] RFID Journal, http://www.rfidjournal.com/article/articleview/841/1/1/ , accessed 24 May 2004

[26] Digi.no, Norwegian information technology webnews, www.digi.no/php.art.php?id=102536, accessed 13 april 2004.

[27] EPCglobal Standards, http://www.epcglobalinc.org/standards_technology/specifications.html , accessed 24 May 2004

[28] RFID Journal, http://www.rfidjournal.com/article/articleview/841/1/1/ , accessed 24 May 2004

[29] AIM, Automatic Identification Manufacturers, www.aimglobal.org , accessed 24 May 2004

[30] EU, http://europa.eu.int/information_society/newsroom/library/theme/isind/text_en.htm , accessed 22 April 2004

[31] ITU Radio regulations, Article 5.150

[32] ERC REC 70-03, http://www.ero.dk/doc98/official/pdf/rec7003e.pdf , accessed 24 May 2004

[33] ERO, European Radiocommunications Office, Electronic Communications Committee, http://www.ero.dk/ecc , accessed 24 May 2004.

[34] ERO, European Radiocommunications Office, http://www.ero.dk/impl-5 , accessed 24 May 2004
[35] ERO, http://www.ero.dk/ , accessed 24 May 2004.

[36] 2002/21/EC, http://www.dcmnr.gov.ie/files/Comms_Reg_Directive_2002_21_%20Framework.pdf , accessed 24 May 2004.

[37] DECISION No 676/2002/EC of the European Perliament and of the Council of 7 March 2004, http://europa.eu.int/information_society/topics/radio_spectrum/docs/pdf/radio_spectrum/decision_6762002/en.pdf , accessed 24 May 2004.

[38] CEPT, www.cept.org/MoU, accessed 24 May 2004.

[39] R&TTE Directive 1999/5/EC, http://www.dare.nl/r&tte_dir_uk.pdf, accessed 24 May 2004.

[40] FCC, Federal Communications Commission, http://www.fcc.gov/

[41] NTIA,National Telecommunications and Information Administration, http://www.ntia.doc.gov/

[42] FCC Radio Spectrum Home page, http://www.fcc.gov/oet/spectrum/

[43] FCC Table of Frequency Allocations, http://www.fcc.gov/oet/spectrum/table/fcctable.pdf , accessed 24 May 2004.

[44] Norwegian Post and Telecommunication Authority, http://www.npt.no/portal/page?_pageid=78,41224&_dad=portal&_schema=PORTAL&p_url=/pt_internet/eng/regulations/index.html , accessed 24 May 2004.

[45] Norwegian Post and Telecommunication Authority, http://www.npt.no/portal/page?_pageid=78,41174&_dad=portal&_schema=PORTAL

[46] Ari Juels, Presentation 15 Nov 2003 at RFID Privacy Workshop at MIT, http://www.rfidprivacy.org/agenda.php

[47] RFID Privacy Workshop at MIT, 15 Nov 2003, Agenda, http://www.rfidprivacy.org/agenda.php

[48] Redprairie, Desember 2003, http://www.redprairie.com/knowledge/PDF_whitepapers/RFID-Just_the_facts.pdf

[49] A. Juels, R. L. Rivest, and M. Szydlo, 2003, http://theory.lcs.mit.edu/~rivest/JuelsRivestSzydlo-TheBlockerTag.pdf

[50] The Privacy Act of 1974, http://www.usdoj.gov/foia/privstat.htm

[51] Directive 95/46/EC, http://europa.eu.int/comm/internal_market/privacy/law_en.htm , accessed 24 May 2004.

[52] Status of Directive 95/46/EC, http://europa.eu.int/comm/internal_market/privacy/law/implementation_en.htm , accessed 24 May 2004.

[53] Norwegian Data Inspectorate, http://www.datatilsynet.no

[54] The Data Inspectorate, Protection of Privacy Repoort 2004.

[55] The Personal Data Act, Personopplysningsloven: http://www.lovdata.no/all/hl-20000414-031.html

[56] The Personla Data Act, Regulation, Personopplysningsforskriften: http://www.lovdata.no/for/sf/aa/xa-20001215-1265.html

[57] RFID Journal, Article, http://www.rfidjournal.com/article/articleprint/810/-1/4/ , accessed 10 March 2004.

[58] Military Information Technology, Online Edition, http://www.mit-kmi.com/archive_article.cfm?DocID=168 ,accessed 15 March 2004.

[59] Trond Johansen, Vermund Lea and Ørnulf Storm, Report IKT4200-2003, RFID Identifikasjon av pasienter og pasientprøver ved Sørlandet sykehus i Arendal.

[60] RFID Journal, 19 May 2003, http://www.rfidjournal.com/article/articleview/431/1/1/ ,accessed 24 May 2004

[61] RFID Journal, 17 March 2004, http://www.rfidjournal.com/article/articleview/834/1/1/ ,accessed 28 April 2004.

[62] RFID Journal, 28 April 2004, http://www.rfidjournal.com/article/articleview/921/1/1/

[63] RFID Journal, 22 April 2004, http://www.rfidjournal.com/article/articleview/901/1/1/

[64] RFID Journal, 27 April 2004, http://www.rfidjournal.com/article/articleview/920/1/1/

[65] Dallas Semiconductors, iButton, http://www.ibutton.com/ , accessed 24 May 2004

[66] Nasjonal Strategi for Informasjonsikkerhet, http://www.dep.no/archive/nhdvedlegg/01/06/Nasjo006.pdf

[67] FIPS140-1, Security Requirements for Cryptographic Modules, http://csrc.nist.gov/cryptval/

[68] Military Information Technology, Online Edition, http://www.mit-kmi.com/print_article.cfm?DocID=351

[69] US DoD, United States Department of Defence, http://www.defenselink.mil/

[70] RFID Journal, 10 Sep 2003, http://www.rfidjournal.com/article/articleview/572/1/1/ ,accessed 24 May 2004.

[71] IEC, International Electrotechnical Commission, http://www.iec.ch/

[72] CIO, Computerworld no 1 – 2004.

[73] Dirk Hahnel and Wolfram Burgard, Univercity of Freiburg.

Appendix

Appendix A - Ongoing ISO RFID standardisation

Appendix A – Ongoing ISO RFID standardisation

Some interesting standards currently worked on are summarised in the tables below. They are all part of the work of several Subcommittees within the ISO Standardisation programme.

JTC1/SC31 – Information technology/Automatic identification and data capture techniques

ISO Number	Description	Stage	Stage date
ISO/IEC FCD 15961	Information technology -- Automatic identification and data capture -- Radio frequency identification (RFID) for item management -- Data protocol: application interface	40.20	6 Nov 2003
ISO/IEC FCD 15962	Information technology -- Automatic identification and data capture techniques -- Radio frequency identification (RFID) for item management -- Data protocol: data encoding rules and logical memory functions	40.20	6 Nov 2003
ISO/IEC FDIS 15963	Information technology -- Radio-frequency identification for item management -- Unique identification for RF tags	50.20	5 April 2004
ISO/IEC FCD 18000-1	Information technology -- Radio-frequency identification for item management -- Part 1: Reference architecture and definition of parameters to be standardized	40.99	13 June 2003
ISO/IEC FCD 18000-2	Information technology -- Radio-frequency identification for item management -- Part 2: Parameters for air interface communications below 135 kHz	50.00	27 April 2004
ISO/IEC FCD 18000-3	Information technology -- Radio-frequency identification for item management -- Part 3: Parameters for air interface communications at 13,56 MHz	40.99	13 June 2003
ISO/IEC FDIS 18000-4	Information technology -- Radio-frequency identification for item management -- Part 4: Parameters for air interface communications at 2,45 GHz	50.20	31 March 2004
ISO/IEC FDIS 18000-6	Information technology -- Radio-frequency identification for item management -- Part 6: Parameters for air interface communications at 860 MHz to 960 MHz	50.20	31 March 2004
ISO/IEC FDIS 18000-7	Information technology -- Radio-frequency identification for item management -- Part 7: Parameters for active air interface communications at 433 MHz	50.20	31 March 2004
ISO/IEC AWI TR 18047-1	Information technology -- Automatic identification and data capture	20.00	27 May 2003

	techniques -- RFID device conformance test methods		
ISO/IEC AWI TR 18047-2	Information technology -- Automatic identification and data capture techniques -- RFID device conformance test methods	20.00	27 May 2003
ISO/IEC DTR 18047-3	Information technology -- Automatic identification and data capture techniques -- RFID device conformance test methods -- Part 3: Test methods for air interface communications at 13.56 MHz	40.99	23 April 2004
ISO/IEC AWI TR 18047-4	Information technology -- Automatic identification and data capture techniques -- RFID device conformance test methods -- Part 4: Test methods for air interface communications at 2,45 GHz	20.00	27 May 2003
ISO/IEC AWI TR 18047-5	Information technology -- Automatic identification and data capture techniques -- RFID device conformance test methods -- Part 5: Test methods for air interface communications at 5.8GHz	20.00	27 May 2003
ISO/IEC AWI TR 18047-6	Information technology -- Automatic identification and data capture techniques -- RFID device conformance test methods -- Part 6: Test methods for air interface communications at 860 - 930 MHz	20.00	27 May 2003
ISO/IEC AWI TR 18047-7	Information technology -- Automatic identification and data capture techniques -- RFID device conformance test methods -- Part 7: Test methods for air interface communications at 433 MHz	20.00	27 May 2003
ISO/IEC FCD 19762-1	Information Technology -- AIDC Techniques -- Harmonized Vocabulary -- Part 1: General Terms Relating to Automatic Identification and Data Capture (AIDC)	40.99	27 Nov 2003
ISO/IEC FCD 19762-2	Information Technology -- AIDC Techniques -- Harmonized Vocabulary -- Part 2: Optically Readable Media (ORM)	40.99	27 Nov 2003
ISO/IEC FCD 19762-3	Information Technology -- AIDC Techniques -- Harmonized Vocabulary -- Part 3: Radio-Frequency Identification (RFID)	40.99	27 Nov 2003
ISO/IEC CD 19789	Information Technology -- ADIC Techniques -- RFID for Item Management -- Application Program Interface	30.60	26 June 2003
ISO/IEC AWI TR 24710	Information Technology AIDC Techniques -- RFID for Item Management -- ISO 18000 Air Interface Communications -- Elementary Tag licence plate functionality for ISO 18000 air interface definitions	20.00	31 July 2003
ISO/IEC AWI TR 24729	Specification of Data Value Domain	20.00	22 March 2004

	Interpretation and guidance in AIDC techniques, including radio spectrum use, for the application of item management standards		

JTC1/SC17 – Information technology/Cards and personal identification

ISO Number	Description	Stage	Stage date
ISO/IEC CD 10373-1	Identification cards -- Test methods -- Part 1: General characteristics	30.60	21 April 2004
ISO/IEC CD 10373-2	Identification cards -- Test methods -- Part 2: Cards with magnetic stripes	30.20	27 Aug 2003
ISO/IEC AWI 14443-1	Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 1: Physical characteristics	20.00	14 Oct 2003
ISO/IEC 14443-2:2001/AWI Amd 1	Higher bit rates for proximity cards (optional bit rates higher than 106 kbit/s for Type A and Type B)	20.00	4 Oct 2002
ISO/IEC 14443-2:2001/CD Amd 2	Bit rates for fc/64, fc/32 and fc/16	30.20	28 July 2003
ISO/IEC 14443-3:2001/FPDAmd 1	Higher bit rates for proximity cards (optional bit rates higher than 106 kbit/s for Type A and Type B)	40.20	17 March 2004
ISO/IEC 14443-4:2001/AWI Amd 1	Higher bit rates for proximity cards (optional bit rates higher than 106 kbit/s for Type A and Type B)	20.00	4 Oct 2002
ISO/IEC AWI 15693-1	Identification cards -- Contactless integrated circuit(s) cards -- Vicinity cards -- Part 1: Physical characteristics	20.00	14 Oct 2003
ISO/IEC AWI 15693-2	Identification cards -- Contactless integrated circuit(s) cards -- Vicinity cards -- Part 2: Air interface and initialization	20.00	14 Oct 2003

TC23/SC19 – Tractors and machinery for agriculture and forestry/Agricultural electronics

ISO Number	Description	Stage	Stage date
ISO/DIS 11784	Radio frequency identification of animals -- Code structure	40.99	7 Nov 2003

TC104/SC4 – Freight containers/Identification and communication

ISO Number	Description	Stage	Stage date
ISO/DIS 18185	Freight containers -- Radio-frequency communication protocol for electronic seals	40.60	14 Nov 2002

TC204 – Intelligent transport systems

ISO Number	Description	Stage	Stage date
ISO/CD TR 14812	Glossary of standard terminologies for the transport information and control sector	30.60	4 Dec 2002
ISO/DIS 14815	Road transport and traffic telematics -- Automatic vehicle and equipment identification -- System specifications	40.60	8 April 2004
ISO/DIS 14816	Road transport and traffic telematics -- Automatic vehicle and equipment identification -- Numbering and data structure	40.60	8 April 2004
ISO/FDIS 14906	Road transport and traffic telematics -- Electronic fee collection -- Application interface definition for dedicated short-range communication	50.60	31 March 2004
ISO/CD TS 14907-1	Road transport and traffic telematics -- Electronic fee collection -- Test procedures for user and fixed equipment -- Part 1: Description of test procedures	30.60	18 March 2004
ISO/DIS 15628	Transport information and control systems (TICS) -- Dedicated Short-Range Communication (DSRC) -- DSRC application layer	40.20	16 May 2003
ISO/DIS 15662	Intelligent transport systems -- Wide area communication -- Protocol management information	40.60	5 Sep 2003
ISO/CD TS 17261	Automatic vehicle and equipment identification -- Intermodal good transport -- Architecture and terminology	30.00	22 April 2004
ISO/AWI 17572	Intelligent transport systems -- Location Referencing	20.00	10 Jan 2003
ISO/CD TS 17574	Road Transport and Traffic Telematics (RTTT) -- Electronic Fee Collection (EFC) System -- Security service framework -- Guidelines for EFC security Protection Profiles	30.60	3 Sep 2003
ISO/CD 17687	Transport Information and Control Systems (TICS) -- General Fleet Management and Commercial Freight Operations -- Data Dictionary and Message Sets for electronic Identification and Monitoring of Hazardous Materials/Dangerous Goods Transportation	30.20	22 Nov 2002
ISO/AWI 22951	Transport information and control systems -- Reference model architecture(s) for the TICS sector -- Data Dictionary and Message Sets for Pre-emption and Prioritisation Signal Systems for Emergency and Public Transport Vehicles (PRESTO)	20.00	5 Dec 2002
ISO/AWI 22952	Transport information and control systems -- Reference model architecture(s) for the TICS sector --	20.00	19 May 2002

	Medium and Long Range Communication Standard Requirements -- An Investigation		
ISO/AWI 24533	Transport information and control systems -- Data dictionary and message set to facilitate the movement of freight and its intermodal transfer -- Road transport information exchanges	20.00	12 March 2003

ISO International harmonized stage codes

STAGE	SUB-STAGE						
	00	20	60	90 Decision			
	Registration	Start of main action	Completion of main action	92 Repeat an earlier phase	93 Repeat current phase	98 Abandon	99 Proceed
00 Preliminary stage	00.00 Proposal for new project received	00.20 Proposal for new project under review	00.60 Review summary circulated			00.98 Proposal for new project abandoned	00.99 Approval to ballot proposal for new project
10 Proposal stage	10.00 Proposal for new project registered	10.20 New project ballot initiated	10.60 Voting summary circulated	10.92 Proposal returned to submitter for further definition		10.98 New project rejected	10.99 New project approved
20 Preparatory stage	20.00 New project registered in TC/SC work programme	20.20 Working draft (WD) study initiated	20.60 Comments summary circulated			20.98 Project deleted	20.99 WD approved for registration as CD
30 Committee stage	30.00 Committee draft (CD) registered	30.20 CD study/ballot initiated	30.60 Comments/ voting summary circulated	30.92 CD referred back to Working Group		30.98 Project deleted	30.99 CD approved for registration as DIS
40 Enquiry stage	40.00 DIS registered	40.20 DIS ballot initiated: *5 months*	40.60 Voting summary dispatched	40.92 Full report circulated: DIS referred back to TC or SC	40.93 Full report circulated: decision for new DIS ballot	40.98 Project deleted	40.99 Full report circulated: DIS approved for registration as FDIS
50 Approval stage	50.00 FDIS registered for formal approval	50.20 FDIS ballot initiated: *2 months*. Proof sent to secretariat	50.60 Voting summary dispatched. Proof returned by secretariat	50.92 FDIS referred back to TC or SC		50.98 Project deleted	50.99 FDIS approved for publication
60 Publication stage	60.00 International Standard under publication		60.60 International Standard published				
90 Review stage		90.20 International Standard under periodical review	90.60 Review summary dispatched	90.92 International Standard to be revised	90.93 International Standard confirmed		90.99 Withdrawal of International Standard proposed by TC or SC
95 Withdrawal stage		95.20 Withdrawal ballot initiated	95.60 Voting summary dispatched	95.92 Decision not to withdraw International Standard			95.99 Withdrawal of International Standard