TDDC03 Projects, Spring 2004

An Introduction to RFID – Information Security and Privacy Concerns

Björn Johansson

Supervisor: David Byers

An Introduction to RFID – Information Security and Privacy Concerns

Björn Johansson
bjojo744@student.liu.se

Abstract

This report is written as part of the course TDDC03 Information Security at Linköping Institute of Technology. It aims to give an introduction to RFID, point out the current and future uses of the technology and to evaluate and discuss the technology from a perspective of information security and privacy with focus on new arising concerns.

1. Introduction

Radio Frequency Identification is yet another step towards fully automatic identification systems. The technology promises faster, reliable and more accurate identification of goods marked with RFID-tags. These are qualities long waited for and furthermore enabling distant out-of-sight identification regardless of bad weather or day-light, the technology gives itself a wide range of uses. The first "old technology" to be (partly) replaced by RFID is the bar code system – RFID can do everything bar codes can and much more [16]. Today, over 5 billion bar codes are scanned daily world-wide [6], [4] and this is just one operation which RFID technology is predicted to take over. RFID supporters claim we are to see an integration of RFID in all businesses – and maybe even where we least expected it to be?

This paper aim to explain why tags initially is to be seen on case level only (except at trial sites) within the driving consumer goods industry and how a basic RFID system is constructed and furthermore why passive RFID-tags are the main concern discussing RFID in terms of information security and privacy.

Hopefully this paper will help the reader to build his or her own understanding of RFID, to enable critical evaluation of the technology and to catch opportunities as well as to avoid threats as the usage of RFID increases around us.

2. Motivation and background

In the world of RFID Walmart [21] is currently the strongest actor pushing the adoption of this new way of identifying everything that can be marked with a tag. Walmart encourages its supplier to adopt the technology by 2005 at the latest for identification at case level [9]. Main competitors to Walmart – e.g. Tesco and Metro group – follow close behind and have do to some extent cooperate in evaluating and implementing RFID at trial sites. The Metro Group operates "next-generation" supermarket in Rheinberg, Germany, with RFID implemented, where benefits of the technology have been seen [6].

Now the actual idea of RFID is nothing new, it has, together with the more know bar coding technology [6], [21], been around since the 60's [22] and the regained interest for RFID has come through the last centuries' amazing technological advances, removing technological hurdles and pushing down prices. With RFID new uses of identification and collection of data about movements of items will be possible and it is thus understandable that major interest is given to issues concerning information security and privacy. Lack of assurance regarding privacy and information security is one of the remaining obstacles for wide spread usage of RFID where e.g. all produced items will be tagged [9]. This can only be done if individuals do not have to worry about forsaking their privacy.

Many issues related to information security and privacy within RFID systems are inherited through using already know technology and methods (e.g. distributed systems, communication of the Internet and wire-less communication). However there are many new issues regarding personal privacy having to be discussed.

Along with the advances of RFID there are many consumer rights and privacy rights groups protesting against trial-sites of RFID and appealing to court for everything from a ban of, to stricter regulations on the use of RFID. The claim is that there is little knowledge about RFID security and privacy flaws and that a better understanding of how large scale RFID-systems will work and look like has to be gained before the technique are integrated in systems where it will affect individuals.

Today RFID is in use in production and assembly sites, in car keys and in home security alarms [18] protecting things of high value. Prices of RFID tags are still too expensive to compete with e.g. bar codes [18] for identification to low cost, but prices are dropping and market analysts believe that the first major roll-outs on case level [6] will take place in 2004-2005. It is about time to learn more about RFID.

3. A RFID system

The goal of a RFID system is to collect information automatically, fast and without errors. There is currently no established standard for the infrastructure of future RFID systems but there are three main components which will be part of all systems [3], [22]:

- **the RFID tags** placed on objects keeping information identifying the host objects,
- **the RFID reader**(s) (including antenna) can both read or write data to the tag, and
- **the data processing system** supporting the read/ write processes and processing the read data.

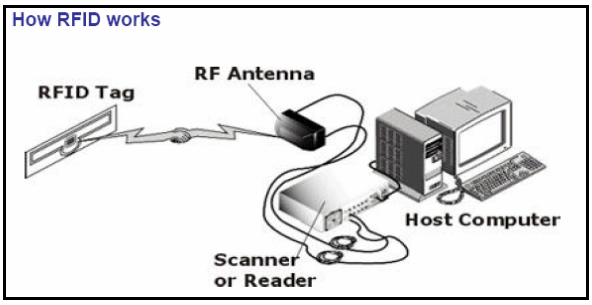


Figure 1: Basic RFID System [13]

A RFID system can pick up signals from several tags at a time with help of anti-collision algorithms and the reader doesn't have to be in line of sight of the object to be identified. A great advantage to bar code systems is that e.g. items in a paper-box can be scanned at once without having to open the box [21], [16] as long as it is within range of the reader.

3.1. Tags

RFID tags come in all different materials and shapes, and typically consist of a microchip with an antenna for picking up and communicating with a reader. When the tag is triggered by a radio signal it will respond by transmitting its unique number [12]. This number is received by the reader and can be looked up in a reference list / database to gain more knowledge about the object identified through the tag's id.

A tag can be powered in different ways and depending on its power source, a tag is classified as an active, passive or semi-passive tag [16]. Active tags are powered by batteries, while passive tags use the incoming signal through induction [12], [4]. Passive tags working without an external power source can remain "alive" for a very long time. Semi-passive tags use batteries for powering the chip in the tag, but using the power of the reader's signal for the actual transmission.

With passive tags, the distance at which communication can take place is determined by the signals' frequency, reader output power, antenna design, and method of powering up the tag. Battery driven (active) tags with their own power sources have not got this problem and can remain in contact with a reader over long distances (hundreds of meter). Passive tags only function in the closer range (at the most a few meters). [4], [16], [3]

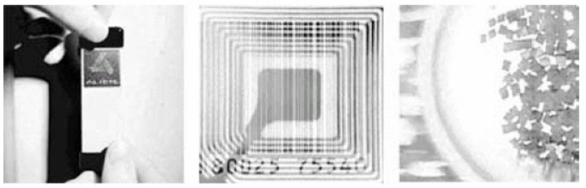
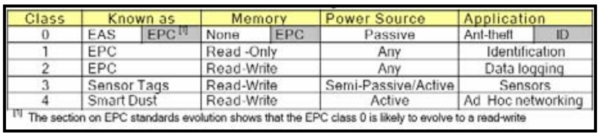


Fig. 1. A passive RFID tag, an RFID tag with a printed barcode, and dust-sized RFID microchips.

Figure 2: Different tags [4]

In an attempt to establish recognised RFID tag standards the EPC global, an association promoting standards governing the RFID technology, has established 5 different classes of tags [13] depending on e.g. their usage, memory type and power source.



Class	Known as	Memory	Power Source	Application
0	EAS EPC [1]	None EPC	Passive	Ant-theft ID
1	EPC	Read -Only	Any	Identification
2	EPC	Read-Write	Any	Data logging
3	Sensor Tags	Read-Write	Semi-Passive/Active	Sensors
4	Smart Dust	Read-Write	Active	Ad Hoc networking

[1] The section on EPC standards evolution shows that the EPC class 0 is likely to evolve to a read-write

Figure 3: Different RFID-tag classes

3.2. Readers

RFID readers continuously send out interrogating radio signals in the search for responding tags. Signals are typically sent out at predetermined frequency bands (see figure 5). The signal will wake up passive tags close by and enable communication with passive as well as active tags. After decoding the signal from the reader as valid the tags will respond. [13], [16], [3]

The distance from which a reader can establish contact with a tag is called the read range and the maximum rate at which data can be read from the tag is the read rate (bits or bytes per second). A stronger powered interrogation signal and a higher frequency for communication increase the range of communication, and then for especially passive tags using the signal for powering itself. [16]

3.3. Data processing system

Due to limitations in transfer rate, range and time of transmission it is crucial that as little information as possible is transmitted between tags and readers. Thus the information stored on a tag (especially passive tags) is often limited to an identifying number only. This value is often called a key-value or the tag's identification number and is passed from the reader to the data processing system.

Such a system has access or contains further information about each item marked with a tag. With a known key-value the system can look for more information about the tagged item.

These systems can be independent systems in closed systems (with no sharing of information with the rest of the world) or networked (where the information about the read tag's host object might not always be held locally). In the case of networked systems or when an item's information is not held locally a scanned tag's key-value can be looked up via the Internet. This is an approach supported by the EPC-concept discussed later in section 5.

In the case of active tags much more information than key-value can be transmitted and stored. With their own power source, active tags can have more advanced (and power consuming) functions built into them. They can for instance be equipped with functionalities for measurements, generating outputs which can be used to initiating actions such as opening doors or other actions in a system connected to the RFID data processing system.

4. Communication in a RFID system

Communication in a RFID system differs a little depending on which kind of tags that are used. Active tags can send out data continuously, while passive tags need a reader's radio signal to power them. Most tags, both passive and active, communicate only when they are interrogated by a transceiver [3].

The range of communication is determined by [27]:

- The power available at the reader
- The power available within the tag to respond
- The environmental conditions and structures [27]

For passive RFID tags read-range can vary from less than a couple of centimetres to at most a couple of meters. Active and self-powered tags can have read-ranges up to several hundred meters [2], [3].

4.1. Inductive coupling and backscatter

Passive tags typically obtain their power from the communication signal through inductive coupling or backscatter [3], [16]. Using the same signal for harvesting energy and communication sets a limit to how long time the transfer of data can go on to the time during which the tag will be powered - often no longer than 400 ms [3].

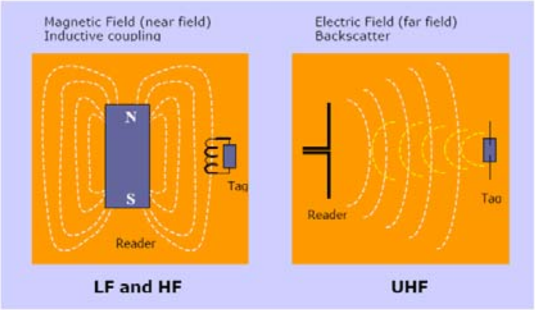


Figure 4: Two ways to transfer energy and information between reader and tag. [13]

Inductive coupling uses the magnetic field generated by the communication signal to induce a current in its coupling element (a coiled antenna and a capacitor). The current induced in the coupling element charges the on-tag capacitor that provides the operating voltage, and power, for the tag. [3] Inductive coupling only works in the near-field of the communication signal since the magnetic field weakens of with increasing distance. [3]

RFID tags using backscatter technology reflect a portion of the radio waves reaching them back to the reader. Tags using backscatter technology can be either passive or active, but either way, they are more expensive than tags that use inductive coupling. [16] For details on backscatter and inductive coupling see [13].

4.2. Frequencies and bandwidths

There are various regulations limiting how information can be sent between readers and tags. Different authorities have different rules all over the world (see [13] page 15-16 for details about frequencies and definitions), but usually RFID operates in what is called Industrial- Scientific-Medical (ISM) bands. It is free to operate in these bands, but the emitted power levels and the side band limits tend to be very strict [3].

Frequency:	Low	High	Ultra High	Microwave
Frequency Range:	<135 KHz	13,56 MHz	860-930 MHz	2,45 GHz
Read range: (Passive tags)	< 0,5 m	~1 m	~4-5 m	~1 m

Figure 5: Definitions of L, H, UH and Microwave frequencies and read ranges for passive tags. [13]

4.3. Data coding and modulation

Two crucial factors for reliable communication of data (represented by ones and zeros) between tags and reader are the encoding of data and its transmission. The combination of coding and modulation schemes determines the bandwidth, integrity, and tag power consumption [3].

There are two dominating categories of codes being used: level codes and transition codes. Level codes represent the bit (the value 1) with the voltage level while transition codes represent different values through a change in voltage level. [3]

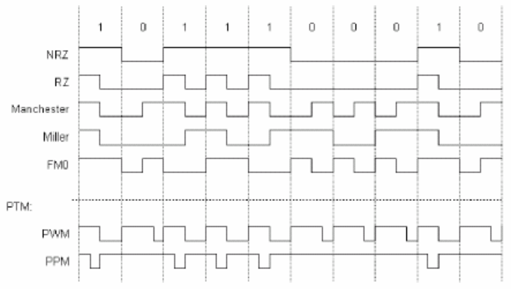


Fig. 1. Examples of several coding schemes.

Figure 6: Different coding schemes. [3]

Pulse Pause Modulation (PPM) code is claimed to be the simplest, and it uses the length between pulses to signal the bit. This code is slow but very easy to implement. Depending on the bandwidth available, most RFID systems use PPM or PWM to communicate from reader to tag and Manchester or NRZ to communicate from tag to reader. [3].

For RFID applications a coding technique must be selected with three considerations in mind:

1. the code must maintain power to the tag as much as possible,
2. the code must not consume too much bandwidth, and
3. the code must permit the detection of collisions. [3]

The data coding scheme determines how the data is represented and how that stream of bits is communicated between the tag and the reader is determined by a modulation scheme. The modulation scheme is based on available power, requirements on reliability and bandwidth restrictions. [3], [16]. The three classes of digital modulation are: Amplitude Shift Keying, Frequency Shift Keying and Phase Shift Keying (PSK) [3], [16]. For more information on modulation please see [3], [16].

4.4. Tag-Anti Collision

Anti-collision is a general term used to cover methods of preventing radio waves from one device to interfere with radio waves from another [16].

When multiple tags respond simultaneously to a reader's signal, their communication signals can interfere with one another. This interference is referred to as a collision and typically results in a failed transmission. In order for a reader to communicate with multiple tags, a method for collision free communication with tags must be employed. These methods are referred to as anti-collision algorithms. An anti-collision algorithm must be employed if an application will typically have more than one tag communicating with a reader at the same time. [3], [23], [16]

The number of tags that can be identified simultaneously depends on the frequency (please see Figure 5 or [13]) and protocol used, and can typically range from 50 tags/ second for HF (high frequency) and up to 200 tags/ second for UHF (ultra high frequency). [13]

4.4.1. Anti-collision algorithms. Based on how tags respond to a reader's signal the anti-collision algorithm is classified as probabilistic or deterministic In probabilistic algorithms, the tags respond at randomly generated times. There are several variations of probabilistic protocols depending on the amount of control the reader has over the tags. [3], [4]

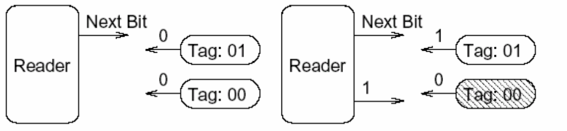


Fig. 5. Silent Tree Walking: The left-hand figure illustrates reading the first bit, which does not collide. The right-hand figure illustrates a collision. To singulate tag 01, the reader responds with "Last Bit" ⊕ "Tag 01" = $0 \oplus 1 = 1$. Tag 01 proceeds, while the shaded tag 00 ceases the protocol.

Figure 7: Tree Walking [4]

A simple deterministic algorithm is the binary tree-walking scheme. The IDs of the tags are all unique and can be seen as leaves of a binary tree. This structure makes it possible to step by step work ones way down to single out individual tags [4]. In this scheme a reader queries all nearby tags for the (firsts or) next bit of their ID number. If the reader detects a collision between two tags, the reader will send a response bit indicating which tags should continue the communication. Each time this happen, the reader goes one level further down in a binary tree. Please see [3] and [4] for detailed descriptions of anti-collision algorithms.

4.5. *Read-Anti Collision*

RFID systems have traditionally been used in sparse applications where readers have been far apart. In future application (e.g. in warehouses or at shop counters) it is foreseen that the density of readers will be much higher. This gives a new problem when signals from one reader can interfere with the signal from another where coverage overlaps. [3]

The solution to a reader collision problem is to allocate frequencies over time to a set of readers and one technique doing this is called time division multiple access (TDMA). In practice a TDMA system makes sure that readers are instructed to read at different times instead of trying to read at the same time. [24], [3], [16]

5. The EPC concept

The EPC concept is the first serious attempt to create a standard for wide-spread use of information generated through RFID systems. It has been developed and implemented to enable all physical objects to be connected in real-time to the Internet by affixing an RFID tag to the object [14]. The four key components of this system are the Electronic Product Code (EPC), the Object Name Service (ONS), the Savant, and the RFID transponders. [3], [13]

EPC is seen to be the next system for pallets and cases over the next five years, and it is already used by Gillette [21] in trial runs. Costs (especially related to passive tags) are the main prohibitive factors stopping EPC from being implemented at the level of individual consumer goods products. [21]

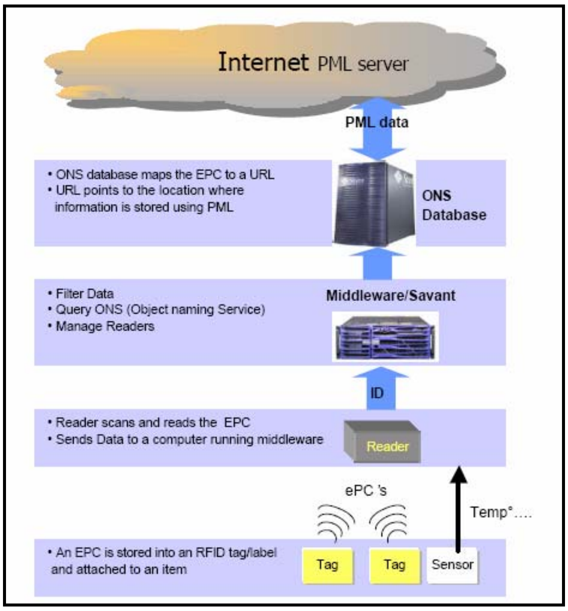

Internet PML server
PML data
• ONS database maps the EPC to a URL
• URL points to the location where information is stored using PML
ONS Database
• Filter Data
• Query ONS (Object naming Service)
• Manage Readers
Middleware/Savant
ID
• Reader scans and reads the EPC
• Sends Data to a computer running middleware
Reader
ePC 's
Temp°....
• An EPC is stored into an RFID tag/label and attached to an item
Tag
Tag
Sensor

Figure 8: Basic steps in the EPC-system infrastructure [13]

5.1. *Electronic Product Code*

The Electronic Product Code (EPC) is an identification scheme designed to enable the unique identification of all physical objects. It is to be seen as a reference value and it is the only data that must be stored on a tag. Once the key value has been retrieved from the tag identifying that unique item, it will function as a pointer to more information for the supporting data management system. [3], [6], [5],[2]

The EPC code is very similar to the UPC (Universal Product Code) in bar codes, and ranges from 64 bits to 256 bits with 4 distinct fields. (See figure 9.) The major difference to bar codes, as pointed out in 2, is that the EPC can distinguish between individual items of the same kind of product. This is very useful in supply chain management [13].

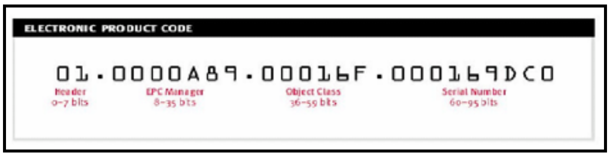


Figure 9: Layout of an EPC which is 96 bits in length [13]

Header (0- 7) bits:	The Header is 8 bits, and defines the length of the code. In this case O1 indicates an EPC type 1 number which is 96 bits in length. The EPC length ranges from 64 to 256 bits.
EPC manager (8- 35) bits	Will typically contain the manufacturer of the product the EPC tag is attached to
Object Class (36-59) bits	Refers to the exact type of product in the same way a an SKU (Stock Keeping Unit)
Serial N umber (60 – 96) bits	Provides a unique identifier for up to 2^96 products [13]

The idea is that each and every manufacturer will get their own identifying number, as well as numbers for their products. For each product group every manufactured item will get its own serial number. With cheaper tag-prices it will be possible to individually mark everything being produced and existing. A 64-bit unique identifier enables approximately 18 thousand trillion items to be market with different values. [8]

5.2. *The Savant*

The Savant is the proposed data management unit. It receives the tag data from the reader, processes it and takes actions. The actions can be to send messages, to call for a look-up of the given tag ID or to filter results when two readers happen to interrogate the same tag. [26], [5], [2] This kind of software agents are very important since no human being will be able to process the flow of information generated by hundreds or even thousands of tags interrogated by several readers at the same time. In a way the Savant works as a buffer. It protects the rest of the system from unwanted data by only letting through requested data. Savants are also expected to be able to detect inconsistencies among tags, check upon readers and to pass on requests to the Object Naming Service (ONS). [13], [3], [25], [5]

5.3. *Object Name Service (ONS)*

The Object Name Service (ONS) receives the request from the Savant containing an EPC. It is now the ONS's task to locate a source of information for the identified object. All items with an EPC-code will have a corresponding entry in the ONS directory with a IP (Internet Protocol) address pointing at a source for more information. This source could be maintained by companies individually or by service providers making sure that their clients' products' data is kept up-to-date, and that entries for new items and product families are entered. At the IP address pointed to by the ONS, data about the particular object is stored using a XML like language called Physical Markup Language, and can be accessed by standard methods like HTTP and SOAP. [13], [5], [16] [3]

The EPC-system will ensure that information of all items identified by EPC is accessible to all interested parties and that this information can be retrieved automatically. To avoid time consuming fetching of data a company can opt to have frequently accessed EPC:s stored locally.

ONS reduces the burden on the transponders, and provides several advantages simultaneously. First, it reduces the memory and power requirements on the tag. Secondly it takes care of a lot of heavy information transmissions and thirdly it makes the system more robust – it is difficult to store and recover information from a failed tag, but it is possible to back up databases. [3]

5.4. *Physical Markup Language*

The proposed physical markup language is designed to give easy access to and make product information stored on numerous servers possible to understand. It is meant to be a universal language and with its help all useful information, static or dynamic data, stored on different servers around the world it to be made retrievable. [14], [16]

The servers keeping all this information are called PML Servers and they direct incoming requests to the right physical markup language (PML) file corresponding to the stated Electronic Product Codes. The manufacturer of an item will be responsible for the maintenance of the PML servers and files containing information about the tagged item. [16]

PML is designed to store any relevant information about a product. For example location, physical properties, composition information and manufacturing and expiry dates. [13]

Today, there is no commercially running EPC system.

6. Security and Privacy

The driving force behind the RFID technique is increased efficiency (in terms of resource usage) through improved, extended and automatic information flows. The technique will enable flows of information never seen before, e.g. information about individual tagged items' whereabouts and with increase transparency suppliers and retailers are to increase competitiveness and consumers will supposedly enjoy better service and greater selection. These are all admirable goals creating a most complex system.

At first it can be hard to grasp the complexity of running a large scale RFID system supported by e.g. the discussed EPC-concept. It builds on most of today's known usage of information technology: servers, clients, distributed networks and databases, authentication, wireless communication etc. Take further into account that these kinds of systems are to integrate IT even further into the process of decision making in businesses (where they ideally are to make sound decisions automatically) and synchronisation of information between businesses, and it is obvious that there will be one or two obstacles in getting it up and running.

With the use of e.g. servers and Internet many vulnerabilities and threats to the systems security and the privacy of the users are inherited. This can for instance be malicious agents faking an innocent PML request over an ONS service or a disgruntled employee adding incorrect product information in the database - causing confusion and damaging the systems integrity.

This chapter will look closer at the privacy and security concerns arising from areas in which RFID distinguishes itself from most current usage of information technology. Discussions about e.g. the utilization of Internet and distributed networks are thus to be found elsewhere.

RFID systems are different from other means of identification because RF communication is non-contact and non-line-of-sight, whereas other means of identification are either contact-based or require line-of-sight. In other words, it is more difficult for the owner/ carrier of a RFIF tag to physically impede communication with the tag. [3]

Tiny (passive) RFID tags can be embedded in all kinds of consumer products and scanned from between a couple of inches to a couple of meters away, revealing information about the product and (potentially) its owner. Today there are tags no bigger than a grain of sand [8] – a Japanese chipmaker has created an RFID microchip sized 0.3 square millimetres [17]. Critics say the technology could reduce or eliminate purchasing anonymity and could even threaten civil liberties. [7], [9], [2]

In [4] the concerns of RFID regarding information security and privacy are summarised in the following way:

"RFID tags may pose security and privacy risks to both organizations and individuals. Unprotected tags may have vulnerabilities to eavesdropping, traffic analysis, spoofing or denial of service. Unauthorized readers may compromise privacy by accessing tags without adequate access control. Even if tag contents are protected, individuals may be tracked through predictable tag responses; essentially a traffic analysis attack violating "location privacy". Spoofing of tags may aid thieves or spies. Saboteurs could threaten the security of systems dependent on RFID technology through denial of service."

6.1. Attacks

If cost is not a problem many privacy and security concerns could easily be mitigated or solved. However, seeking an opportunity to implement RFID on a large scale anything increasing the price will be avoided – in other words extra security measures will be avoided. Indeed there will always be more expensive tags with all features available – strong encryption of data, robust physical tamper proof design etc. Though it is not to be taken for granted that these tags always will be safe [3],[4] – on the questions what kind of things people do to break into RFID chips and what can be done to prevent this, Scott Mc Gregor of Philips Semiconductor had the following answer [18]:

"They put them in cold liquids, bombard them with gamma rays, do what's called differential power analysis. Basically, they've noticed that the chip uses a slightly different amount of power if you get an incorrect digit than if you get a correct digit, and they try to break the code that way. They take the chip apart and try to discover the password on the logic components. To counter that, we use temperature sensors and radiation sensors on our chips. We have all kinds of voltage protection, so they can't monkey around with that. The logic is randomly distributed. We have coding on the chip…that's really hard to scrape off without permanently damaging the chip." [18]

However low-cost passive tags ("low-cost" today implies that they are passive) often lack all these protection mechanism and functionalities and are thus the main threat for privacy and information security violations. They are unable to host more advanced protection mechanisms due to e.g. their design with power inductions from the readers radio signal. These tags' ID can be read by not to sophisticated readers and there is not a clear message from the industry whether these tags will be left alive or not after leaving e.g. a store. [8] This situation is rightfully a major concern for consumer privacy activists, and the possible effects of low-cost tags responding with information to any request ought to be considered by each and everyone in contact with such RFID systems or thinking about setting up such a system.

6.1.1. Counterfeiting and spoofing. If one is able to read or intercept data being written into a tag which uniquely identifies or certifies a product the system is open to counterfeiting and spoofing. Once the data is known, similar read/ write tags could be updated with the authentic data. In this way it is possible to make similar cheaper copies of the initially tagged item, and thereafter counterfeit its authenticity. [13]

By spoofing valid tags, a thief could fool automated checkout or security systems. It would also be possible to rewrite tags on expensive items with spoofed data from cheaper items. For industries this could be a concern since saboteurs could disrupt supply chains by redirecting or faking flow of goods by corrupting a large batch of tags. [4] On the other hand RFID tags could also be used as seals of authenticity in documents, designer products, and currency and in this way discourage forgery. [3] The European central bank is for instance considering embedding RFID tags into banknotes by 2005. [8]

6.1.2. Denial of service. An infrastructure dependent on RFID tags may be vulnerable to denial of service attacks. The communication between the tags and the readers as well as between the Savant and ONS are just two examples of possible sore spots. Delayed identification of an item might cause critical states of an operation, or e.g. let a faulty item pass where is should not.

One countermeasure proposed to ensure privacy of the individual is the blocker tags (further discussed in section 6.2.3), sending out random signals – could become a threat if applied as the signature "Nick" proposes:

"Just wait till someone gets hold of one of RSA's little blocking devices and plugs it into a more powerful transmitter. You then have a rather nice denial of service tool. Imaging dropping them amongst the jumpers at Marks and Spencers, 'Nick'" [10]

Such an attack would cause the entire system to fail. The readers would not be able to distinguish between the fakes “tags” signalled from the “blocker tag” and the items in the store. A too heavy load on the systems readers might as well cause the system to fail.

A more sophisticated approach is to broadcast noise on the response frequency of the tags of a known system. This is likely to jam the signal, preventing the reader from identifying the tag. [12]

6.1.3. Eavesdropping. Efforts are being made to protect consumer privacy by securing information at all levels of data exchange. A major difference between RFID and say magnetic stripe technology (as is used on bank cards) is that it operates over air. Basically it can be said that the very properties making RFID technology attractive in terms of efficiency make it vulnerable to eavesdropping [4]. The risk of eavesdropping or intercepting transmitted data is well recognized, as is the risk of someone using a concealed reader. Both of these risks are greatly reduced through the design of appropriate over-the-air protocols and data encryption methods. [22]

In addition, a reader changing frequency rapidly makes it more difficult for an eavesdropping reader to follow the main reader exactly. If the hopping sequence is random the communication will be very difficult to follow. [22] This is also something which can be implemented with passive low-cost tags.

6.1.4. Silent Tree Walking. Eavesdroppers may monitor a communication channel from hundreds of meters in attempts to derive tag contents and information about the object it identifies. In the communication between reader and tags different anti-collision schemes are used. Of particular concern is the binary tree walking anti-collision algorithm, because the reader broadcasts each bit of the sought object’s tag’s ID. [4]

Silent Tree Walking stands for a class of "bugging" devices that might be deployed by criminals to attack RFID tags reading operations to disrupt a business. Note that the Silent Tree Walking breach of security is only possible if the use anti-collision algorithm is tree walking. [11]

A Silent Tree Walking device could be used by unauthorized persons to discover RFID tag numbers. It acts by covertly monitoring the dialogue between the authorised Reader and present tags. [11]

Through carefully monitoring the dialog between a read and tags and could through the queries from the reader follow the reader’s path down the tree structure and finally learn the ID of a scanned tag. The fact that the bugging device never transmits during tag reading means that the presence of one or more Silent Tree Walkers would be almost impossible to detect. [11]

6.1.5. Information leakage. Consumer rights organisations worry about the possibility that e.g. authorities or thieves will be able to monitor people’s personal belongings through small embedded RFID microchips remaining active after purchase. [1], [12]

Considering the security properties of passive tags, this is in theory well possible. Each tag contains a unique identifier such as the earlier discussed EPC-code and is, and will be, easily scanned by a standard reader. In other words the tracking of tag holders as well as the reading of a tag’s stored information is possible as long as the tag is within reading range. No authentication is needed.

An obvious solution to this problem would be to cut of all tags after purchase and to destroy them. However, they might not always be easy to find. KSW-Microtec, a German company, has invented washable RFID tags designed to be sewn into clothing. [8]

To sum things up individuals carrying items with unsecured tags are vulnerable to privacy violations. There is nothing stopping evil minds from scanning you from top till toe which is a clear threat towards confidentiality and personal privacy. As mentioned earlier it is also possible to counterfeit tags. This could be done to one of your tags, or a counterfeited tag could be placed into a “normal” product. Then problems could arise if you are registered to possess something you shouldn’t owe. This is a clear threat to your personal integrity.

With unique ID numbers on each item all around the world, and databases keeping records on all EPC and RFID related movements, privacy is at great danger from many perspectives. It may be possible to aggregate data to find out facts about your person, your prescriptions, bad habits or your whereabouts as long as enough items can be connected to you at the point of sales or later. [2].

Figure 10: Monitoring of people's personal belongings [19]

6.1.6. ID tracing. Another important privacy concern is the tracking of individuals by RFID tags – the violation of “location privacy”. A tag reader at a fixed location can track RFID-labelled clothes or banknotes carried by people passing by. With data from readers at different locations it will be possible to track movements, social interactions, and financial transactions. A tag embedded in a shoe could serve as a de facto identifier for the person wearing it.

As an example concerns over location privacy were recently raised when a major tire manufacturer began embedding RFID tags into all their products [24]. With readers at different exits along a high-way one could trace a person’s movements.

If personal identity is linked with unique RFID tag numbers, individuals could be profiled and tracked without their knowledge or consent. [2] Even if the tags only contain product codes rather than unique serial numbers, individuals could still be tracked by the “constellation” of products they carry. [4], [2], [11]

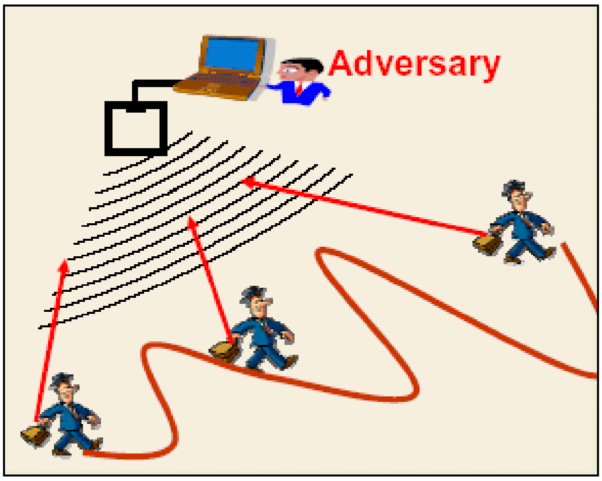


Figure 11: Tracking of individuals by the tags they carry [19]

6.2. *Possible countermeasures*

Looking at the basic components of a RFID system, readers (or Savants rather) have to reject suspicious tag replies with abnormal response times or signal power levels. This can serve as a countermeasure to spoofing attempts of active tags, or detection of blockertags.

As mentioned under 6.1.3 readers could take use of frequency hopping to avoid session hijacking interrogating passive tags. Since there is no need for synchronisation between readers and passive tags, which follow the reader frequency and signal, coping with random hops are trivial for the tag. However they will be very hard to follow.[4]

Regarding privacy most concerns would seemingly go away with the deletion of the unique serial numbers at the point of sale. Tags would still contain bar code equivalent information but it would no longer be possible to connect unique item to an individual.

6.2.1. Hash function. There are proposals were a hash-enabled tags contain a portion of memory reserved for a “meta-ID” and operates in either an unlocked or locked state. While unlocked, the full functionality and memory of the tag are available to anyone in the interrogation zone. [3]

To lock a tag, the owner computes a hash value of a random key and sends it to the tag as a lock value. In turn, the tag stores the lock value in the meta-ID memory location and enters the locked state. While locked, a tag responds to all queries with the current meta-ID value and restricts all other functionality. To unlock a tag, the owner sends the original key value to the tag. The tag then hashes this value and compares it to the lock stored under the meta-ID. If the values match, the tag unlocks itself. [3]

Access control to tag contents is restricted to key holders, but individuals may both locate and physically disable tags since tags always respond to queries through denial or acceptance.

Lacking authentication exposes tags to man-in-the-middle attacks since an attacker can query tags for meta-IDs, rebroadcast those values to a legitimate reader, and later unlock the tags with the reader’s response keys. Many key-less car entry systems currently possess the same vulnerability. [3]

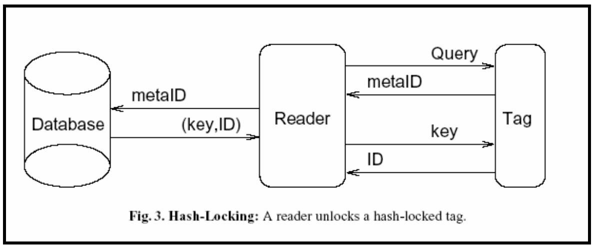


Figure 12: Hash-Locking, a reader unlocks a hash-locked tag [4]

The hash-lock scheme only requires implementing a hash function on the tag and managing keys on the back-end. This is a relatively low-cost requirement and may be economical in the near future. Unfortunately, since the metaID acts as an identifier, tracking of individuals is possible under this scheme. [4]

To learn more about hash-locking and random hash-locking scheme see [3], [4] and [19].

6.2.2. Silent Tree Walking. In retail RFID tag system, a Silent Tree Walking (see section 6.1.4) receiver could be hidden near the Point of Sale reader at the checkout. Screening of vulnerable readers to stop signals reaching the listening "Silent Tree Walker" is one possible countermeasure. However, this would be difficult to do even with fixed readers. It would make the reader ineffective for some legitimate reading operations. [11]

An alternative countermeasure is also not to use the tree walking anti-collision algorithm, but instead use e.g. a time slot transponder identification using e.g. the "ALOHA" protocol. [11] It has the characteristic of separating tags for reading or writing in time rather than with code. With this method it will be impossible for a "Silent Tree Walker" to trace items ID's from just listening to the reader's transmissions. This is because in reading operations the reader does not need to transmit any part of the tag's identity number in order to effectively single out a tag in its close surroundings [11]

6.2.3. Blocker tags. Blocker tags do so far only exist in theory and it is uncertain how well they would function in reality. [2] Theoretically a blocker tag will disturb the transmission between a selected group of tags or all tags in a certain area. It could be embedded in a bag or a pocket to prevent their content (containing or marked with tags) to be revealed. Wearing blocker tags would thus protect you from having your belongings scanned by unauthorized people.

A blocker tags can e.g. works in the way that they respond to readers' queries with first a "yes" and then a "no" vice versa. Consequently, in a binary tree search the reader thinks that every "leaf" on the tree is populated with a tag number. As a result the search time for reading ID numbers from present tags tends to be very long (inventory data obtained will also be valueless). [11]

That such tags will be banned on for instance airports and public buildings, are very likely since one could use them to hide guns or other hazardous items. [2]

6.2.4. Self destruct command and secret keys. A built-in self destruction command would make it possible for individuals to destroy tags electronically and to permanently enable identification of e.g. the bought item through the tag [3]. This would stop any unwanted leakage of information. [4] Or as expressed in [11] - "Dead tags don't talk" [11].

The problem with this approach would be that not anyone can be allowed to destroy tags. This right has to be controlled and the action must not be trivial. Otherwise evil minds could go into a warehouse and destroy all tags on items stored, or steal items, destroy the tags and claim that they belong to them.

This situation calls for "secret keys" used to destroy tags; one key for each tag and item. The administration would be massive, but it is a good way for trying to stop unauthorized killing of tags [18]. The actual killing of a tag could be through disconnecting the antenna or intentionally short circuiting a fuse. [4]

With the development of EPC schemes the "kill" function is certainly something which has to be offered to consumers and especially if RFID is to be implemented on item level of consumer goods or their packaging. When it comes to larger items, such as refrigerators, the easiest thing will still probably be to manually remove and destroy the tag. [22]

A remaining concern from privacy groups though is that tracking is still possible within the store before the point of sale. [2] Furthermore it can be discussed how the actual "killing of tags" will be done and where it is supposed to take place. It might not be feasible to do it at the point of sales (if it can not be fully automatic) due to time limitations. If the option is to go to "killer kiosks" some people might not bother or afford it if the service is not free of charge.

According to [8] Wal-Mart says that they will disable tags at checkout, while Gillette Vice President Dick Cantwell said that its RFID tags would be disabled at the cash register only if the consumer chooses to "opt out" and asks for the tags to be turned off. [8]

6.2.5. Closed System. With a closed system e.g. company internal id numbers could be used. However this would go against the idea of a universal id system enabling flows of goods between companies and their logistics chains. On the other hand, if cars, persons or items are to be tagged and traced within set geographic areas and the information generated through their e.g. movement are only to be used within a company internally there is no need for standard codes. This would just enable eavesdroppers to listen after standard codes on the other side of the fence, tracking movements and possibly predicting actions. [2]

7. Consumer groups and movements

Different consumer and privacy groups have tried to take legal action in attempts to get the case with RFID tags on consumer goods tried in court. They have demanded further regulations controlling the usage of RFID [15],[9]. The main concern is that the technology will abuse individuals' privacy and thus the activists call for:

- an openness regarding RFID systems structure and functions,
- that no tags are used without a clear purpose,
- that the collection of information is limited avoiding aggregation of data,
- accountability for the implementation of the technology and the collected data,
- any private information carried by a tag has to be protected appropriately, e.g. through encryption,

- killing or removing tags shall be easy – tags may not be hidden - and
- security safeguards protecting the system's e.g. databases and transmissions have to be installed [2], [3]

The bottom line is that people involved in the discussion on the consumer groups' side are seriously concern that "It's possible to set up these systems so that there is no privacy anywhere" and that we in the future can be tracked through what we are "eating and wearing". [8], [1]

Activists' groups have also taken direct action again RFID through protests. Such a campaign forced Tesco to end a tagging trial at a Cambridge store in August, 2003 [7] and in March [2003] the company Benetton had to call of ideas of marking clothes after consumer groups had launched a worldwide boycott of its products. [9]

7.1. Accepted uses of RFID

However there are some uses of RFID which even the activists' groups believe can be carried out without causing loss of personal integrity and privacy, or where the use of RFID might even be preferable. Such cases are for instances:

- Tracking of pharmaceuticals

This could be done to ensure that these sensitive substances are not tampered with, and that they could be called back if needed. [18], [2]

- Tracking of manufactured goods from the manufacturer to where they will be shelved for sale.

Using RFID will help keeping track of the flow of goods and make sure goods are not lost. A major standpoint for these organisations is that tags are not to be used on item level [2] – keeping previous discussions of this paper in mind it is not hard to understand why. In the Walmart launch in 2005 RFID tags are only going to be used on palettes and cases, not on the actual items, keeping them away from the consumers [1].

Until appropriate solutions are developed and agreed upon it is improper to subject consumers to the dangers of RFID technology through item-level consumer product tagging [2]. For the foreseen use of tags on consumer goods level a group of activists groups have proposed four guidelines to companies tagging individual items:[8]:

- Notify the customer
- Disable tags by default at point of sales
- Place RFID tags on container instead of on the actual item when possible.
- Don't hid tags – they should be visible and easily removable [18]

Only few voices [9] raise the demand that RFID should be abandoned completely [7]. This is not very likely to happen since the technology is already successfully employed in closed system e.g. for tracking of pharmaceuticals [9] and in the car industry where the benefits of such a system are evident.

In [18] RFID is furthermore predicted to play an important role in most of today's situation involving keys or access rights.

8. Conclusions and summary

With strong actors such as Walmart, expecting an annual return of investment of $1.3-$1.5 billion from reducing supply chain related costs [21] taking use of RFID, a global adoption of the technology is seemingly hard to inhibit. Nevertheless it is important to distinguish between different RFID systems and how they are used.

Most e.g. manufacturing processes and control processes using RFID systems work with high value items, and thus motivating more expensive (often active) tags costing more than US$1.00. For this price it is possible to include basic cryptographic functions and tamper-resistant packaging ensuring information security and individuals' privacy. However the passive tags foreseen to be used at the major roll outs don't have any of these features – we are left with situations described in section 6.

In other words it is the use of low-cost passive tags which is of primary concern as we get closer to the price range of US$0.05-US$0.10 [8], [21] enabling cost effective wider uses. At this price range, providing strong cryptographic primitives is currently not a realistic option. [4], [3]

These low-cost RFID systems are, of necessity, very resource limited, and the extreme cost pressures make the design of RFID systems a highly coupled problem with sensitive trade-offs. Every company is faced with this trade-off between cheaper unsecured tags, and the potential security risks they entail. [13] Even the simplest security features cost, and will therefore have a negative impact on the final tag price [13]

The challenge will be to develop a complete open standards-based system that enables the design and manufacture of RFID systems [3] with the adoption of e.g. symmetric encryption and public key algorithms remaining in the low-cost price range (US$0.05-0.10) for its tags. Such passive RFID devices are expected to be reality first in a couple of years. [3] This prediction is certainly also one of the privacy and consumer rights groups' major concerns. Will the global players and technology pushers Walmart, Gillette, Tesco etc. recognise the problems connected with too simple passive RFID tags and wait till tagging of (consumer goods) items can be done in a safe way?

Currently RFID tags are only going to be used on pallet level and e.g. Gillette and Walmart claim that *"At this point in time, the tag is useless beyond the store shelf. There is no value and no harm in the tag outside the distribution channel. There is no way it can be read or that (the) data would be at all meaningful to anyone."* [8] This statement is probably true at the moment, but again what will happen if a standard (e.g. EPC) is spread, RFID (passive) tags are being used on item level and readers are available?

The conclusion can only be that RFID is going to be something big – when it will happen and which criteria that have to be fulfilled for it to be fully accepted and reliable are questions still open for discussion. With increased volumes through use on pallets prices will drop making tagging economically possible on item level and then it is important that one carefully makes sure that a possibility to save a cent in the cost of a tag is not done of the expense of the security and privacy of its future users. [3]

Most likely we are going to see a mixture of solutions and implementations of the RFID technology. Some stores will inform about the use of RFID, and some companies might make it a cooperate policy not to use RFID on item level, others will give you clear instructions how to kill your tags upon exiting their store.

One of the more interesting questions will probably be if the large community can be bothered about insecure RFID tags and how RFID can compromise individual privacy, when they at the same time will be enjoying different benefits of RFID systems.

In favour of RFID it has to be said that there is a great potential for companies and individuals. Companies will increase their competitiveness and individuals will e.g. enjoy more comfort as well as more accurate and faster service. Furthermore it can strengthen trust between parties in a supply chain through making the flow of goods more transparent – it will be possible track the goods in real time.

But to be kept in mind is that accepting this technology will mean trade-offs for all involved parties and one has to carefully consider what this possible trade-off is and might entail.

Having now learnt about the fundamentals of RFID, known problems and countermeasures, the reader will hopefully be able to make such judgements and recognise opportunities where an RFID system can be of use without conflicting with personal privacy and information security.

9. References

[1] Gilbert, A., "Privacy advocates call for RFID regulation", http://zdnet.com.com/2100-1105-5065388, C|net News.com, 2003-08-18, available: 2004-03-31

[2] "Position Statement on the Use of RFID on Consumer Products", http://cdt.org/privacy/031114rfid.pdf, CASPIAN et al., 2003-11-14, available: 2004-05-01

[3] Sarma S., Weis S. et al., "RFID Systems and Security and Privacy Implications", http://citeseer.ist.psu.edu/sarma02rfid.html, Auto-ID Center, available: 2004-05-01

[4] Stephen A., Sanjay E., et al., "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", http://citeseer.ist.psu.edu/sarma02rfid.html, Auto-ID Center, available: 2004-05-01

[5] "Auto-ID Center Opens Demo Lab", http://216.121.131.129/article/articleprint/22/-1/1/ , RFID Journal, 2002-07-11, 2004-03-31

[6] "Intel rethinking RFID?", http://www.theregister.co.uk/content/archive/34877.html , The Register, 2004-01-14, available: 2004-04-04

[7] Leyden, J., "Moratorium on RFID chips urged", http://www.theregister.co.uk/content/55/34109.html, The Register, 2003-11-20, available: 2004-03-31

[8] McCullagh, D., "RFID tags: Big Brother in small packages", http://news.com.com/2010-12-980325.html, C|Net News.Com, 2003-01-13, available: 2004-04-01

[9] Garfinkel, L. S., "The Trouble with RFID", http://www.thenation.com/doc.mhtml?i=20040216&s=garfinkel, The Nation, 2004-02-03, available: 2004-03-31

[10] Sherriff, L., "Tinfoil hats to retail with RFID tags?", http://www.theregister.co.uk/content/35/36038.html, The Register, 2004-03-05, available: 2004-04-04

[11] Hawkes P., "On Tree Creepers and their control", http://www.eurotag.org/article/Tree_creepers.pdf, available: 2004-05-01

[12] Kipling Z., "RFID info", http://lists.indymedia.org/pipermail/imc-cambridge/2003-August/000276.html, [Imc-cambridge], 2003-08-04, available: 2004-05-01

[13] "A Basic Introduction to RFID Technology and its uses in the Supply Chain", , http://www.idii.com/wp/LaranRFID.pdf, Laran RFID, January 2004, available: 2004-05-01

[14] "EPC: Components (Part 2 of a series)", http://www.aimglobal.org/technologies/rfid/resources/articles/June03/EPCpart2.htm, Association for Automatic Identification and Mobility, available: 2004-03-31

[15] Rutner S., Waller M., “A practical look at RFID”, http://manufacturing.net/scm/index.asp?layout=articlePrint&articleID=CA85844/, 2004-01-01, available: 2004-03-31

[16] “Glossary of RFID Terms”, http://www.rfidjournal.com/article/articleview/208, RFID Journal, available: 2004-03-31

[17] “Hitachi Unveils Smallest RFID Chip”, http://216.121.131.129/article/articleprint/337/-1/1/, RFID Journal, 2003-03-14, available: 2004-03-31

[18] “Like It or Not, RFID Is Coming”, http://www.businessweek.com:/print/technology/content/mar2004/tc20040318_7698_tc121.htm?tc, BusinessWeek online, 2004-03-18, available: 2004-03-31

[19] Ohkubo M., Koutarou S., Kinoshita S., “Cryptographic Approach to ‘Privacy-Friendly’ Tags”, NTT Laboratories, Workshop material, 2003-11-15

[20] “Security Access and Convenience for Express Parcel Courier”, http://www.aimglobal.org/technologies/rfid/casestudiy/TIfedex.htm, Association for Automatic Identification and Mobility, available: 2004-03-31

[21] Shim, R., “Walmart to throw its weight behind RFID”, http://news.com.com/2102-1022_3-1013767.html, C|Net News.Com, 2003-06-05, available: 2004-03-31

[22] “Are you new to RFID?”, http://www.afeindustries.com/rfid_faq.htm, RFID News, available: 2004-03-31

[23] Stevenson P., “Tag collision?”, http://www.rfidtalk.com/showthread.php?threadid=34/, RFID Talk, 2003-05-11, available: 2004-03-31

[24] Stevenson P., “Reader collision”, http://www.rfidtalk.com/showthread.php?threadid=35/, RFID Talk, 2003-04-11, available: 2004-03-31

[25] Stevenson P., “intelligent software agents”, http://www.rfidtalk.com/showthread.php?threadid=19/, RFID Talk, 2003-03-11, available: 2004-03-31

[26] “RFID Technological Risks”, http://www.rfidtalk.com/showthread.php?threadid=270/, RFID Talk, 2004-03-03, available: 2004-03-31

[27] “Radio Frequency Identification RFID – A basic primer”, http://www.aimglobal.org/technologies/rfid/resources/RFIDPrimer.pdf/, AIM, 2001-08-23, available: 2004-05-01