

# Student Sample Technical Report

Report on

**RFID**

**Radio Frequency Identification**

This report is an actual student assessment task, reproduced with the kind permission of the student.



# Table of contents

1	INTRODUCTION .....	3
2	WHAT IS RFID? .....	3
3	HOW DOES RFID WORK? .....	4
3.1	Communication process .....	4
3.2	Energy Supply .....	5
3.3	Technology weaknesses .....	5
4	DATA PROTECTION AND PRIVACY .....	6
5	AREAS OF APPLICATION .....	6
5.1	German passport .....	6
6	CONCLUSION .....	7
7	LIST OF FIGURES .....	9
8	REFERENCES .....	9

## 1 Introduction

In this day and age fast and secure identification has become a major issue for both industry and governments. Governments are particularly interested in improving identification processes; industry, on the other hand, concentrates on the automation of their processes.

For this reason many technologies have been developed to automate and assist in the process of identification. The most common identification system used by industry is the barcode system which is still found on many products at the supermarket. However, its functionality is very limited, since it can neither be read from a distance nor save any further data. For that reason a new system called RFID (Radio Frequency Identification) has been developed which implements this feature and opens many new possibilities. Using this technology it is now possible to read many items at the same time and to even store additional data on it such as finger prints for passports.

However, not everyone is happy with this new development. RFID opponents such as customer protection groups, argue that the protection of privacy is neglected. They are afraid the system could be easily used to create movement or customer profiles without the customer knowing it.

This report aims to explain how the RFID technology works and how it is currently used by industry and governments. Security and privacy aspects will also be discussed, since they are very important to whether this technology will be accepted by the market or not.

## 2 What is RFID?

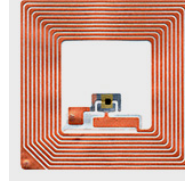
RFID (Radio Frequency Identification) is a system used to accelerate and automate identification and localization processes using radio frequency technology as communication method.

An RFID system typically consists of the following components:

- **Transponder (Transmitter – Responder)**  
Also called RFID label or smart label, consisting of microchip, antenna, case and a capacitor or battery to store energy. It is able to save and send data
- **Reading/Writing device**  
Antenna which is able to initiate communication with the transponder and to read / write data to the RFID chip
- **IT infrastructure**  
Integrated into a server and computer networking environment database information can be accessed from the server (e.g. prices or verification of documents)



**Figure 1 - RFID read- / writing device**  
Source: RVB Systems Group, 2006



**Figure 2 - RFID transponder including antenna and microchip**  
Source: Texas Instruments, 2006

In comparison to older systems, such as the barcode, RFID systems have two major advantages. Firstly data transfer between the transponder and the reading device can now operate wireless without visual contact using radio frequency technology. Secondly the functionality of the chip is expandable, since there are many diverse types on the market implementing different features. The most important and common feature is data storage. The majority of chips can store up to 72 kB of data which is more than enough for most purposes. Some more advanced chips also implement further security features such as data encryption and digital signatures. Thereby data content can be protected from unauthorized access (confidentiality) and modification (integrity) and can be attributed to a source or owner (authenticity) e.g. passport picture - holder.

The size of a transponder is strongly influenced by the size of the antenna which is the largest element. Furthermore the antenna defines the broadcasting frequency as well as the reading distance

Examples of "real life" applications can be found in Chapter 5.

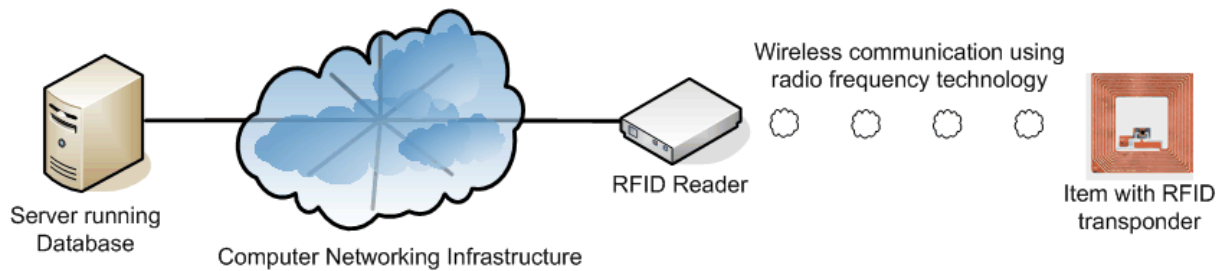
### 3 How does RFID work? <sup>1</sup>

#### 3.1 Communication process

The communication process (represented in Figure 3) is initiated by the reading device. This device creates an electromagnetic field with the same frequency that the transponder is listening to. The signal is received by the transponders antenna creating an induction current which activates the microchip. Passive transponders will also use the induction to charge their capacitor; active ones use their battery as energy source.

---

<sup>1</sup> Garfinkel, S 2006, 'RFID – Applications, Security and Privacy', Addison-Wesley, Boston



**Figure 3 - Data communication in an RFID system**

Source: RFID transponder by Texas Instruments, 2006; others by Kogler, 2006

Once activated the transponder is now ready to receive commands from the reading device. Data can be read from the chip to compare with database entries stored on the server.

### 3.2 Energy Supply

There are two different kinds of transponders; active and passive which differ in their energy supply and reading range.

Since **passive components** do not have their own energy supply they have to be provided with sufficient energy through the communication process. A so-called "continuous wave" has to be provided by the reading device to keep the transponder running. Due to the fact that magnetic field strength decreases with the square of the distance of the transponder, passive components are very limited in reading range. In fact they can only be read from less than one meter.

**Active components**, on the other hand, utilize their own energy supply using a battery. Once they are activated by induction of the magnetic field they don't need any further energy source from the field. Thereby they can be read from greater distances. A state of the art transponder is able to radio from up to 10 meters and greater reading distances, using higher frequencies are currently being developed. Active components are a lot more expensive than passive.

### 3.3 Technology weaknesses

One of the greatest challenges from a technology point of view is that the RFID chips can not be read under certain conditions. For example the transponder is very susceptible to metal objects in its neighbourhood, since metal strongly reflects the electromagnetic field of the read device. Water contact can also prevent communication, since the magnetic field is absorbed by water.

## 4 Data protection and privacy

With the increasing ability of computers to automate the collection of data, protection and privacy have become increasingly more important. Ideally every customer should be able to decide individually which data about them is saved by an organization after a purchase is made. Unfortunately, however, data protection and privacy issues in RFID systems have been neglected so far. On some occasions transponders have been used without the customers knowing it. For instance the Metro group<sup>2</sup> has inserted a transponder into its new customer card, but customers are only alerted to this in the fine print. Furthermore there is currently no means to effectively deactivate transponders. In some areas of applications the transponder can be destroyed using a simple microwave, but doing so is not advisable, since there is a danger of fire. In addition a verification of the customer if the transponder is deactivated is mostly not possible.

## 5 Areas of application

RFID systems are becoming more and more interesting to industry and governments. According to Quack<sup>3</sup> (2006) 600 million RFID transponders have been sold in 2005 and this number is expected to increase to 1.3 billion in 2006.

Based on a survey conducted by the company IDTechEx, Raghu Das<sup>4</sup> (2005) points out, that the largest investments into this new technology come from the car and security industry, which are already using it intensively.

The following section will introduce a 'real life' example.

### 5.1 German passport

The German government<sup>5</sup> has implemented improved security features for all passports issued after 1. November 2005. These features are realized in an RFID transponder which is embedded into the document. So

---

<sup>2</sup> Alhazred, A 2004, 'Metro withdraws customer cards', Quintessenz, <http://www.quintessenz.org/d/000100002835> [Accessed 9.10.2006]

<sup>3</sup> Quack, K 2006, 'RFID boom has only just begun', <http://www.computerwoche.de/nachrichten/579177/index.html>, Computerwoche [Accessed 4.10.2006]

<sup>4</sup> Das, R 2005, 'RFID tag sales in 2005 - how many and where', IDTechEx, <http://www.idtechex.com/products/en/articles/00000398.asp>, [Accessed 4.10.2006]

<sup>5</sup> Bundesministerium des Inneren (ministry of internal affairs), 2006, 'Questions and answers about the e-Passport', [http://www.bmi.bund.de/cln\\_012/nn\\_122688/Internet/Content/Themen/Informationsgesellschaft/Einzelseiten/ePass\\_\\_Biometrie/Biometrie\\_\\_FAQ.html](http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Themen/Informationsgesellschaft/Einzelseiten/ePass__Biometrie/Biometrie__FAQ.html), [Accessed 3.10.2006]

far only a picture of the passport holder and a security code is saved on the chip. However, having a capacity of 72 kB, it is designed to store further biometrical characteristics such as finger prints and iris scans in the near future. In addition to the large capacity, sophisticated security features are implemented.



**Figure 4 – German Passport**  
Source: Bundesdruckerei, 2006

For instance data communication between the reading device and transponder is encrypted using a cryptographic coprocessor. Moreover electronic signatures such as checksums prevent unauthorized modifications.

## 6 Conclusion

RFID is setting a new standard in automation. Since new features can be added to the chip, this technology is very well prepared for future applications. Especially branches of industries that rely strongly on logistics or are specialize in automation profit significantly from these new developments as they accelerate processes as well as decrease expenses. Furthermore sophisticated security systems can be developed which will be interesting for security services as well as governments.

However, the number of critics and opponents is continually increasing also. Customer protection organizations in particular protest that the protection of personal data is neglected. In fact in some cases they have even been successful. As already stated the Metro group tried to introduce new customer cards with RFID transponders in 200; however, having received massive complaints, they removed the transponders shortly after their beginning.

Only time will tell how this technology may be used in the future. Improvements to the major problem areas such as protection of personal data, as well as more transparency for customers, would contribute to a better image and acceptance on the market.



## 7 List of figures

Figure 1 - RFID read- / writing device, RVB Systems Group, <http://www.barcode-solutions.com/>

Figure 2 - RFID transponder including antenna and microchip, Tsukada, K.,  
<http://mobiquitous.com/pub/sd200502.html>

Figure 3 - Data communication in an RFID system, source: Kogler, O

Figure 4 – German Passport, Bundesdruckerei,  
[http://www.bundesdruckerei.de/pics/4\\_presse/fotoarchiv/aktuelle\\_fotos/050601\\_BMI\\_ePass\\_ohne.jpg](http://www.bundesdruckerei.de/pics/4_presse/fotoarchiv/aktuelle_fotos/050601_BMI_ePass_ohne.jpg)

## 8 References

Alhazred, A 2004, 'Metro withdraws customer cards', Quintessenz,  
<http://www.quintessenz.org/d/000100002835> [Accessed 9.10.2006]

Bundesministerium des Inneren (ministry of internal affairs), 2006, 'Questions and answers about the e-Passport',  
[http://www.bmi.bund.de/cln\\_012/nn\\_122688/Internet/Content/Themen/Informationsgesellschaft/Einzelseiten/ePass\\_Biometrie/Biometrie\\_FAQ.html](http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Themen/Informationsgesellschaft/Einzelseiten/ePass_Biometrie/Biometrie_FAQ.html), [Accessed 3.10.2006]

Das, R 2005, 'RFID tag sales in 2005 - how many and where', IDTechEx,  
<http://www.idtechex.com/products/en/articles/00000398.asp>, [Accessed 4.10.2006]

Garfinkel, S 2006, 'RFID – Applications, Security and Privacy', Addison-Wesley, Boston

Quack, K 2006, 'RFID boom has only just begun', Computerwoche,  
<http://www.computerwoche.de/nachrichten/579177/index.html>, [Accessed 4.10.2006]