Technische Universität Darmstadt
Dept. of Computer Science

RFID Seminar

Winter Term 2005/2006

Supervisors:

K. Sachs, P. Guerrero*, M. Cilia and A. P. Buchmann

{sachs, guerrero, cilia, buchmann}@dvs1.informatik.tu-darmstadt.de

Databases and Distributed Systems Group

* GK Enabling Technologies for E-Commerce

Preface

Radio Frequency Identification (RFID) is becoming more and more important. A wide range of applications is being influenced by this technology, like supply chain management (SCM). The usage of RFID in SCM allows a better track and trace of items, and supermarkets are currently demanding their suppliers to deliver tagged shipments. RFID is being investigated in very different areas, like security (e.g. for access control), health care (e.g. to identify a patient including some personal information like blood group), and food supplies (e.g. to trace the meat in the supermarket back to the animal). This seminar explores the current state and future deployment of RFID and familiar technologies and applications.

March 2006

Kai Sachs,
Pablo Guerrero,
Mariano Cilia,
Alejandro Buchmann;
Darmstadt, Germany

Table of Contents

Introduction to EPCglobal

Tsvetan Penev and Daniel Hofmann

Databases and Distributed Systems Group
Dept. of Computer Science, TU Darmstadt, Germany

Abstract. This paper gives a short introduction to the work of the EPCglobal Inc. as a world-wide amalgamation of companies, as well as the standards and services it provides. It describes the EPCglobal Architecture Framework, which is a collection of standards for hardware, software and data interfaces used by the RFID technology, whereas not all parts of the Architecture Framework will be extensively described. In exchange it focuses special parts and furthermore addresses the services defined by the EPCglobal Inc.

1 Introduction to EPCglobal

This chapter should give a short introduction to the work of the EPCglobal Inc. for giving you an idea about the organization. For a more detailed description, please see the references [EPC] for further reading.

The EPCglobal Inc. is a global organization that is made up of the GS1 (formerly known as EAN International) and the GS1 US (formerly known as the Uniform Code Council, Inc.). It is a neutral non-for-profit organization responsible for worldwide valid standards concerning the EPC (Electronic Product Code) used in current RFID technologies, especially the identification of information in the supply chain of a company. EPCglobal standards are made for defining standardized interfaces, not to deliver any kind of implementation. So developers should be encouraged to build innovative products and systems, which ensure interoperability through the given standards. EPCglobal is an open organization working as a community, where end users are integrated in the development and may have influence on the acquired standards.

The EPCglobal provides a multiplicity of services regarding companies that use RFID technology for improvements of their supply chain, for example the following services are provided:

- assignment, maintenance and registration of EPC Manager Numbers
- participation in the development
- access to standards, research and specifications
- training and education
- the EPCglobal Network which provides services for cross-business data exchange between the EPCglobal Network suppliers

1.1 Basics on RFID

RFID stands for Radio Frequency Identification and can be explained as a kind of wireless data transfer. RFID Tags are very small devices consisting of a microchip and an antenna and are used for storage of an identification number (see EPC). These tags can be read by RFID readers through radio waves, where the RFID readers are then transmitting the ID numbers to a special - depending on the according purpose or company - business information systems using RFID middleware.

1.2 Members

Numerating the members of the EPCglobal Network would be giving a list of the who-is-who of global players. Since the standards of EPCglobal are concerning all producers and traders it is a long list and not part of this paper. For giving an idea, we name the following members:

- Procter & Gamble
- Hewlett Packard
- WalMart
- DHL
- Cisco
- Etc.

1.3 Architecture Framework Overview

The EPCglobal Architecture Framework consists of three main parts; here we will give a short overview over these parts which are geared to activities of the EPCglobal Subscribers. As the Architecture Framework is the main part of this paper, it will be described more detailed later.

Fig. 1 shows the three main activities of the EPCglobal Architecture Framework where each of it involves a number standards defined by EPCglobal. Here we introduce each of these activities and the corresponding standards.

- EPC Physical Object Exchange Standards
  The standards defined in this section are used for the delivering of physical objects; this is used when an object (e.g. a trade good) is delivered from one supplier to another. This means an object which can be identified by an EPC is being shipped, received, etc.
  The corresponding standards are listed below, see references for further reading:
  - UHF Class 0 Gen 1 RF Protocol [UHFC0]
  - UHF Class 1 Gen 1 RF Protocol [UHFC1G1]
  - HF Class 1 Gen 1 Tag Protocol [HFC1]
  - UHF Class 1 Gen 2 Tag Protocol [UHFC1G1]
  - EPC Tag Data Specification [TDS]

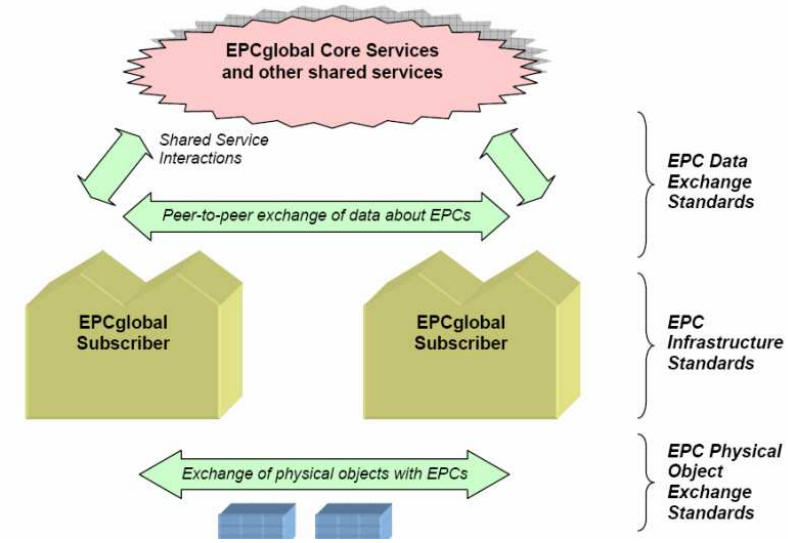

Fig. 1. EPCglobal Architecture Framework Overview [EPC p.8]

- EPC Data Exchange
  This provides peer-to-peer connection between EPCglobal Subscribers and so transparency for the subscribers e.g. concerning movement of objects. So information between the subscribers can be shared for common interests and businesses.
  The corresponding standards are listed below, see references for further reading:
  - EPCIS Data Specification [EPCIS]
  - EPCIS Query Interface [EPCIS]
  - EPCIS ONS [ONS]
  - EPCIS Discovery
  - Subscriber Authentication
- EPC Infrastructure
  While the EPC Data Exchange is defining standards for data exchange between subscribers, the EPC Infrastructure defines standards for using EPC within the subscribers business. This means that the subscriber gathers and records EPC data for his internal systems, which includes the creation of new EPC's and tracking the movement of objects.
  The corresponding standards are listed below, see references for further reading:
  - EPC Tag Data Specification [TDS]
  - Reader Protocol [RP]
  - Reader Management [RM]
  - Tag Data Translation [TDT]

- Application Level Events (ALE) [ALE]
- EPCIS Capture Interface [EPCIS]
- EPCIS Data Specification [EPCIS]

While these standards may appear to be a very inflexible system for handling of EPC's, the EPCglobal Architecture Framework is designed to give subscribers a helpful tool regarding the use of EPC's. It is meant to be an open system giving a wide range of options to fit the respective needs of the corresponding business.

1.4 Goals

Setting up EPCglobal Inc. as an international organization for creating standards for RFID was done to reach following goals [EPC p. 11ff]:

- o facilitate the data exchange between trading partners by setting up data and information exchange standards as a basis of cross-enterprise exchange
- o encourage innovation through standardized interfaces
- o setting up global standards
- o setting up an open system by developing within a community and as a result to secure free and open rights
- o platform independence
- o scalability and extensibility
- o security
- o privacy
- o integration and compatibility for existing architectures and standards

2 Introduction to EPCglobal - Technical principles

2.1 EPC

The Electronic Product Code (EPC) is the number saved on the RFID Tags to identify them reading the code with an RFID Reader. The EPC assigned to one object is a globally unique number on the RFID Tag. It is a binary number with a length of 96 bits. There are two more versions using 64 and 256 bits, the 64 bit version is used for a short time to offer cheap RFID Tags. The 256 bit version is currently not needed as there is no demand for it at the moment. Here we will introduce you to the version consisting of 96 bits (EPC-96), see table 1.

Element	Header	Filter	Partition	Company Prefix	Item Reference	Serial Number
Bits	8	3	3	20-40	24-4	38

Table 1. Design of the EPC

The header (which includes the fields Header, Filter and Partition) is used to identify the EPC-Version. The lengths of Company Prefix and Item Reference depend on the information stored in the Partition field.

The Company Prefix is used to identify the producer and the Item Reference, which is also called the Object Class is used to identify the product. The EPC so far is comparable with the EAN number, which is used nowadays.

The last field is used to store the serial number of each single object.

2.2 EPC Manager & EPC Manager Number

The assignment of the EPC to physical objects is one of the fields of activities of EPCglobal. The assignment is organized in a decentralized structure, so that there are several Issuing Agencies qualified assigning EPC number blocks to subscribers. The subscriber is then in a position to act as EPC Manager, which means that he can assign the EPC from a given block to objects.

This is done by issuing the EPC Manager a so called EPC Manager Number with that the EPC Manager can derive several EPC's and associate them with an object. With creating EPC's by an EPC Manager Number the EPC Manager has two responsibilities:

- ensure that uniqueness remains in place
- maintenance of the Object Name Service (ONS), which is used for global lookup operations to get information about the objects (see ONS in chapter 3.8)

2.3 EPC Information Services (EPCIS)

EPCIS is the central system for data exchange between EPCglobal subscribers. It is used for the query of data concerning EPC's to provide an information system to authorized trading partners. For example, it provides transparency about localization of physical objects or quantified information; this data can be categorized in Static Data (does not change over the life of a physical object), Transactional Data (grows and changes over the life of a physical object) and Business Transaction Observations as follows:

Class-level Static Data
Data which is the same for all objects of a given object class, e.g. a product may be such an object class.
Instance-level Static Data
Data which is different for the objects within an object class, this could be for example the date of manufacture.
Transactional Data for Instance Observations
Records events that occur during the life of an EPC regarding the information about time, location, business process step and the EPC. For example: "EPC X was shipped from location X on 17th Jan 2006 at 5pm".

Transactional Data for Quantity Observations
To measure the quantity of objects of an object class, regarding the time, location, object class, quantity and business process step of an EPC. For example: "100 instances of EPC X arrived at the storehouse on 18th Jan 2006 at 10am".
Business Transaction Observations
Records associations between EPC's and a business transaction. For example: "Pallet with EPC X was shipped to location Y at 12pm in order to fulfil the purchase order #Z of company C".

The components of EPCIS will be described more detailed in the following chapter.

3 EPCglobal Architecture Framework

The EPCglobal Architecture Framework differs between roles and interfaces of the EPCglobal Architecture Framework. Roles are hardware or software components performing a respective task. Interfaces interlink to roles using a standardized method which are in this context EPCglobal standards. In this chapter we will have a closer look to these components and give an overview over the EPCglobal Architecture Framework.

Figure 2 shows the breadth of the EPCglobal Architecture Framework.

3.1 Short Introduction

Since the focus of this paper is on higher level components of the EPCglobal Architecture Framework, there will only be a short introduction for the following components.

i. RFID Tag (Role)
Contains the EPC code which can be read by a RFID Reader using the Tag Protocol.

ii. EPC Tag Data Specification (Interface)
Defines the structure of the Electronic Product Code and specific coding schemes.

iii. Tag Protocol (Interface)
Responsible for communication between the RFID Reader and one or more tags, additionally this means the selection of a tag if more than one is reachable. This protocol is standardized by EPCglobal in the UHF Class 1 Gen 2 tag protocol. [UHFC1G2]

iv. RFID Reader (Role)
Reads the EPC of a reachable Tag and uses the Reader Protocol to transfer it to a host application. Depending on the application environment the RFID Reader may provide additional features commanded by a host application such

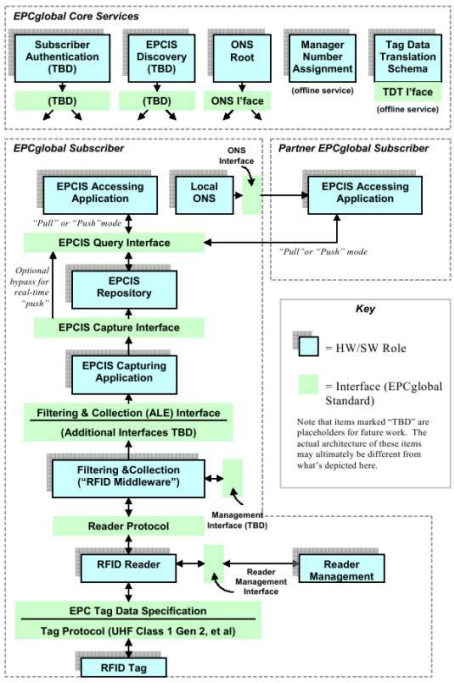

Fig. 2. EPCglobal Architecture Framework, Components and Roles [EPC p.34]

as writing EPC to a tag, kill a tag, lock a tag, etc.

v. Reader Protocol (Interface)
The Reader Protocol provides interfaces to access the RFID Reader for sending commands to the reader and receiving results from it. The commands could be used for operations on the tags (e.g. reading and writing) but also for reader management function (e.g. for configuring and updating the reader, gathering statistics).

vi. Reader Management Interface (Interface)
Provides means to manage the RFID Reader. This could be configuration tasks as updating, controlling tasks as enabling or disabling of antennas or features and information querying, such as reading the readers identity or monitoring the operational status e.g. connectivity.

vii. Reader Management (Role)
This is used for management of a RFID reader. This could be status monitoring, reader configuration management and functions like discovery, power consump-

tion etc.

viii. Filtering & Collection (Role)
This is used for the coordination of activities of one or more RFID readers. Primarily this means handling of possible radio-frequency interferences that could appear if RFID readers use the same physical space.

The raw RFID tag data is received and transformed to a more suitable format for further processing. Filtering in this context means tasks as for example eliminating duplicates, filtering a specific object class and discard not matching objects, counting, and so on. It is also used for management tasks if for example many readers and antennas are present and it is required to collect and activate each reader for itself to prevent interferences.

The Filtering & Collection Role has many responsibilities; unfortunately it is not really specified by EPCglobal yet.

3.2 Filtering & Collection Interface (Interface)

This chapter describes the Application Level Event (ALE) Interface as defined by EPCglobal. It is based on the specification published by EPCglobal in September 2005 [ALE].

The ALE interface provides independence between the components of the EPCglobal Architecture Framework that acquire raw data, filter and count that data and applications that use the data by defining standardized interfaces. The benefit is that applications do not need to be changed, if for example an RFID Reader is exchanged for a newer, faster one.

ALE works on raw EPC data it gets from a component residing at a lower level in the architecture, e.g. from one or more RFID Reader within an event cycle, which may consist of one or more read cycles. (See next paragraph for an example on read an event cycles.) It edits the data (Filtering & Collection) and generates a so called report about the event cycle which then is transferred to the application business logic (see Fig. 3 for a visualization of report generation).

Reports generated by ALE may make a variety of statements about the read EPC's. These could be quiet simple statements for example the list of EPC's, a range of EPC's or the number of EPC's. The reports can also contain more complex information like information about EPC groups (object classes), so grouping has to be done using the specific information in the EPC. For example it is often not needed to know the specific serials numbers, but the number of items of a product on a pallet. In this example, within an event cycle information about the tags (which has been read within multiple read cycles) is collected so that the report "Number of items on a pallet" can be generated.

ALE is also responsible for activating readers that should make EPC data available. Since it is undesirable that some kind of reader-associated information like serial numbers, IP addresses etc. is used for selecting a reader because of maintenance tasks, ALE introduces the notion of "logical reader". For example "DockDoor42" could be used for naming a specific reader using logical readers.

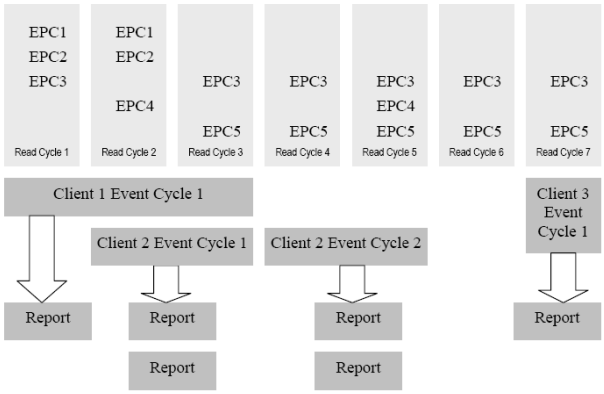

Fig. 3. ALE Report Generation [ALE p.11]

EPCglobal has defined an extensive ALE API, which is described very detailed in the ALE specification paper [ALE].

3.3 EPCIS Capturing Application

The next node in the diagram before is EPCIS Capturing Application (that is the shaded box right above Filtering & Collection (ALE) Interface, and being shaded means that it is a role and not an interface). Now what is the EPCIS Capturing Application responsible for? It monitors how some lower EPC elements function, combines that information with other sources of information, and thus provides business relevant information about the execution of a particular step in a business process.

There are a couple of responsibilities that EPCIS Capturing Application has. One of them is to be aware of EPC-related business events and to deliver that information as EPCIS data. It is also possible to acquire data from multiple information sources first and then to recognize that as an individual EPCIS event. EPC data can be collected by means of human input, barcode data, through the Filtering&Collection Interface or simply from other software systems. It was also noted that in the future versions of the Filtering&Collection Interface, the EPCIS Capturing Interface may have the responsibility to control other devices and write RFID tags as well.

A good example of what the EPCIS Capturing Application is responsible for is a conveyor system, where it plays the role of a coordinator who receives information about certain Filtering&Collection events and takes corrective actions whenever necessary or for instance sends that information to a human operator. It can also coordinate the loading of a whole shipment in which case this would probably involve not one but many Filtering&Collection events. Another example is when we have “smart shelves”. In this case we have periodic

observations about the objects that enter or leave the shelves so there is generally no difference between a Filtering&Collection event and an EPCIS event, since the EPCIS Capturing Application only routes the information from the Filtering&Collection Interface to the EPCIS Repository.

3.4 EPCIS Capture Interface

Now at this level we have our EPCIS data generated by the EPCIS Capturing Application and we want that data to be forwarded to the other grains in the infrastructure. The EPCIS Capture Interface is the one that defines how this EPCIS data is to be routed to the EPCIS Repository or to the EPCIS Accessing Application of some partner. The transmitted data in question above is actually a statement that approximately says that at some particular point in time, at some place, a number of objects(meaning tagged units) have been aggregated to some other object. The information generated at the level of the EPCIS Capturing Application can be also routed such that to skip the EPCIS Repository and directly provide that information to the EPCIS Query Interface, depending on which mode of transfer is the EPCIS Query Interface set to.

3.5 EPCIS Repository

This role in the EPC Architecture Framework speaks for itself and as one can easily guess it deals with storage. The EPCIS Repository is software that is responsible for storing EPCIS events that have been generated by potentially many EPCIS Capturing Applications. Thus, it makes the information available for later query by the EPCIS Accessing Applications(meaning the EPCIS Accessing Applications of some Partners or the EPCIS Accessing Application of the same Subscriber who is in possession of the Repository).

3.6 EPCIS Query Interface

The EPCIS Query Interface is a very important grain in the chain, because it has to be reliable and to provide quick access to the desired information or deny access. Whenever a Partner issues a query request to a foreign(another Partner's) EPCIS Query Interface the Partner should authenticate himself before the query takes place. The EPCIS Query Interface is the grain that should provide means for mutual authentication for the two parties. After the authentication process has finished it should decide whether to give full access to the requested data, a limited view of it or deny access at all. The only way an EPCIS Accessing Application can request EPCIS data from the Repository or the EPCIS Capturing Application is by means of the EPCIS Query Interface. So generally a Partner has to authenticate himself before receiving any data and then with the help of the EPCIS Query Interface query the database and obtain the result of the query, which is formatted according to the EPCIS Data Specification. Last but not least, the EPCIS Query Interface can support two types of data transfer, either pull or push.

3.7 EPCIS Accessing Application

One step higher than the EPCIS Query Interface lays the EPCIS Accessing Application (Role), which has a number of responsibilities. If we assume that we have two Partners that are already part of the EPCglobal Network and they want to exchange data, we have a situation that is similar to what is depicted in the diagram. Now the EPCIS Accessing Application (Role) is an application that is specific to the Partner EPCglobal Subscriber, who is generally interested about information concerning a particular EPC. The EPCIS Accessing Application is the grain responsible for choosing a way how to find the data in question. It can obtain the requested data in a couple of ways.

First, if we are in the two partner model, the EPCIS Accessing Application will actually know in advance that the information that it is looking for resides on the other partner. The network address of the other party's EPCIS service is usually exchanged beforehand as a part of a business agreement.

Secondly, the EPCIS Accessing Application can find the information that it is looking for using the so called method of "following the chain". The idea can be illustrated using a model with three EPCglobal Subscribers (A, B and C). We assume that partner A and partner B know each other and also that B and C know themselves (know means that they know each other's network address of the EPCIS service they provide). However, partner A requires information from partner C whose address it does not know. But A knows B and B knows C, so when A obtains information how to reach B it also learns how to reach C's service and that is called "following the chain".

But following the chain is not very efficient in a more complicated network, so it works only in limited scenarios. The EPCIS Accessing Application has, however yet another way for obtaining information about a specific EPC and that is by using the Object Naming Service (ONS) to find the network address of the EPCIS service of the EPCglobal Subscriber who happens to be the EPC Manager of the questioned object. The next section will give a more insight into the ONS service and hopefully clarify things.

So far the techniques above deal with situations where the Partner EPCglobal Subscriber is interested only about information that is provided from the EPC Manager of the object. But in reality one would like to know some other information when a particular package that is tagged travels through a number of Partner EPCglobal Subscribers before it reaches it's final destination. In this case, "following the chain" is again not applicable since in a multi-party supply chain the participants are not known in advance.

As a whole the EPCIS Accessing Application has a number of other responsibilities, such as warehouse management, shipping and receiving, historical throughput analysis and some other connected with the EPC data.

3.8 Object Naming Service (ONS)

i. Local ONS(Role)

The Object Naming Service can in general be thought of as a service which

accepts as input an EPC and returns as output the address of the EPCIS service given by the EPC Manager of the EPC in question. Conceptually, a request to the Object Naming Service involves using the ONS Root and the Local ONS but the details for the first service are going to be discussed later.

Now the idea for ONS was to be a global lookup service, at least conceptually, but as one can easily guess it is not practical to be implemented that way, both due to scalability issues and the fact that each EPC Manager organization has to provide and update information about all its object classes in a shared database. To cope with these problems another model for implementation was offered, namely structuring the ONS as a hierarchical service. It is architected as an application of the Internet Domain Name Service or more commonly known as DNS. Even so structured, however, the Object Naming Service does not allow different entries for different serial numbers of the same object class. Also the former schemes SSCC and GIAI that don't have fields corresponding to the object class, discussed earlier, are not addressed in the ONS specification. But on the other hand, the ONS different object classes as separate even if they are given by the same EPC Manager. The reason is that different object classes that are even under the authority of the same EPC Manager can have information that is offered by different EPCIS services(meaning different network addresses of the service).

Now let's take and example and assume that an EPCglobal Subscriber wishes to locate a particular EPCIS service. First it has to consult the Root ONS (which is controlled by EPCglobal), which in tern will give a pointer to the Local ONS service of the EPC Manager organization of the EPC in question. After that the Local ONS completes the request by giving the address of the EPCIS service in question.

As it was stated earlier ONS is implemented as an application of DNS and by a convention an EPC is converted to an Internet Domain Name in the onsepc.com domain. This implies a couple of things. First, the Root ONS service and the Local ONS service can be realized as a number of independent servers just like DNS provides us with the possibility (when we setup our network) to list as a provider of DNS service not only one but a say two DNS servers. This means that we should enjoy a greater level of scalability and reliability. Actually the true root of ONS resides in the worldwide DNS root service. Apart from that, the ONS service uses cashing as well (like DNS does), so the most frequently accessed entries are cashed locally and that means that each ONS lookup could possibly involve consulting only one ONS service. (For further info see RFC1034, RFC1035 and ONS1.0)

ii. ONS Interface

The Object Naming Service Interface provides just the means and regulates how one can reference an EPCIS service provided by the EPC Manager of a specific EPC. (Normative reference ONS 1.0)

4 Core Services

4.1 ONS Root

As a continuation of what we talked about above comes the ONS Root core service. Like we said, this is the place where an ONS lookup starts. After that the remainder of the lookup is forwarded to the local ONS, which is operated by the EPC Manager of the requested EPC. If there is no local ONS to which the lookup to be forwarded to, the Root ONS fulfills the request. Last but not least the Root ONS provides lookup service for the 64-bit Manager Index values as specified in the EPC Tag Data Specification 1.1.

4.2 Manager Number Assignment

In order to have unique EPCs for each object class (unique serial item numbers are not applicable due to the significant difficulty that one would have to keep an updated, real-time database for each single item) and to distribute the load of assigning EPCs over the subscribers, EPCglobal assigns EPC Manager Numbers to each EPCglobal Subscriber. From there on each Subscriber is responsible alone for assigning different object class numbers and if necessary serial numbers. Uniqueness is insured by default sort to say, because the EPC Manager Number is just the first couple of bits which comprise the EPC itself and then each Subscriber can allocate the rest of the bits to designate different object classes and unique serial numbers (if necessary) but keeping the same prefix (the EPC Manager Number). Ensuring uniqueness by maintaining unique EPC Manager Numbers is a task for the Manager Number Assignment core service. It is also the one that issues EPC Manager Numbers on request by EPC Subscribers.

4.3 Tag Data Translation Schema and Tag Data Translation Interface

The Tag Data Translation Interface simply defines how the data encoded in the EPC is transformed between different EPC encodings defined by the EPC Tag Data Specification. Now the Tag Data Translation Schema is the one that gives the machine-readable file where it is defined how to translate between different EPC encodings. EPC global only provides end-users with the file, so that components of their infrastructure can become aware of new EPC formats.

4.4 EPCIS Discovery

This core service is not yet a defined part of the EPCglobal Architecture but based on some analysis of use cases it is believed that there is a need for such service. It is not clear now how this will be defined or whether it will be realized as a number of EPCglobal Core Services. It is merely a placeholder and marks the need of such a service and the responsibilities it will have when implemented.

In a multi-party supply chain, where a number of EPC Subscriber can have information about a specific EPC but the identities of those Subscribers are not known in advance, how can we query that information. That will be a responsibility of the EPCIS Discovery service. It will have to provide cache for EPCIS data and probably have to deal with authorization and policies about who has access to the data.

4.5 Subscriber Authentication

This core service is also only a placeholder and a field of intensive future work, since authentication and security are, as I see, probably the major set back for the whole idea, since people are suspicious and cherish their privacy. The list of responsibilities for this service is of course not complete but some of them include:

1. Authenticating the identity of each EPCglobal Subscriber.
2. Manufacturing credentials for one EPCglobal Subscriber so they can authenticate themselves even if they haven't met before.
3. Authenticate participation in network services by validating the EPCglobal Subscription.

There may be some other responsibilities that may arise in the development process but the need for authentication is substantial. It has to be implemented in such a way that each EPCglobal Subscriber has to be able to authenticate himself by other EPCglobal Subscribers even if they haven't met before. It would be best if they can just register once with a central authority and from there on can authenticate by any other subscriber.

5 Summary

The adoption of the EPCglobal Network is gaining gradually popularity. It is still in its early stages now, but there are a number of pilot projects generally in the Fast Moving Consumer Goods industry where the new technology is being tested and the results are promising. Tagging is now at the level of pallets and cases, not on items yet, because just like any other innovation, adoption of the EPCglobal Network needs time for the business community to see the benefits out of it by such test projects. After all, each businessman needs to be convinced that the money that he or she is investing is not going to be wasted for nothing. Luckily, the benefits that EPCglobal promises from the adoption of the new technology that involves the usage of EPC and RFID (Radio Frequency Identification) are quite tempting both for consumers and manufacturers. Today a number of industries are researching and implementing components of the EPCglobal Network, that have been approved before by the EPCglobal Community. There has been a rigorous research going on lately in the area but there are some issues that need to be addressed. You can see those easily as they are marked with the letters TBD in the given diagram at the beginning of this document.

They are defined as placeholders for now, because analysis is currently underway and it may very well be that all services envisioned to be presented by a single TBD node may be split among a couple of new nodes. The good thing about it is, however, that EPCglobal standards development process is an open one and EPCglobal Subscribers are tightly involved in the development. This means that development is more effective and addresses exactly the issues that need to be addressed, since no one is better acquainted with the problems that producers have than producers themselves. So, EPCglobal Subscribers with the necessary knowledge in the field are joining the working groups and creating new standards.

Yet another good thing about the design of the EPCglobal Architecture, which will make it even more appealing to the public, is that it recognizes the need for platform independent specifications. This means that the EPCglobal Architecture Framework can be implemented on different software and hardware platforms. Thus hardware and software companies will be provoked and there will be a great competition amongst them, which on the other hand means that the cost for these software and hardware components will inevitably drop after their ubiquitous adoption.

There is still, however, a great deal of work that needs to be done before the entire EPCglobal Architecture Framework is properly defined. Issues like Security, Subscriber Authentication EPCIS Discovery service are still under construction and even though the people on the front line (EPCglobal Subscribers), who have to face problems for the first time, are the same people that participate in the definition and implementation process, there will be at least about a year before the EPCglobal Architecture Framework is completely defined.

6 References

All documents published by EPCglobal Inc. Documents [RP], [RM], [TDT] and [EPCIS] are working drafts and therefore not published yet.

[EPC] EPCglobal Architecture Framework Version 1.0 (July 1st 2005),
http://www.epcglobalinc.org/standards_technology/Final-epcglobal-arch-20050701.pdf
[ALE] Application Level Event (ALE) Specification Version 1.0 (September 15th 2005),
http://www.epcglobalinc.org/standards_technology/EPCglobal_ApplicationALE_Specification_v112-2005.pdf
[UHFC1G2] Class 1 Generation 2 UHF Air Interface Protocol Standard Version 1.0.9 (January 2005),
http://www.epcglobalinc.org/standards_technology/EPCglobal2UHFRFIDProtocolV109122005.pdf
[UHFC0] 900 MHz Class 0 Radio Frequency (RF) Identification Tag Specification (February 23rd 2003),
http://www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class0.pdf
[UHFC1G1] 860MHz – 930 MHz Class 1 Radio Frequency (RF) Identification Tag Radio Frequency & Logical Communication Interface Specification (November 14th 2002),
http://www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class1.pdf

[HFC1] 13.56 MHz ISM Band Class 1 Radio Frequency (RF) Identification Tag Interface Specification (February 1st 2003),
http://www.epcglobalinc.org/standards_technology/Secure/v1.0/HF-Class1.pdf
[TDS] EPC Tag Data Standard Version 1.1 rev 1.27 (May 10th 2005),
http://www.epcglobalinc.org/standards_technology/EPC_TDS_1%201_Rev_1%2027_Ratification_final%201-2006.pdf
[RP] EPCglobal, Reader Protocol 1.0, EPCglobal Working Draft (March 2005)
[RM] F.A. Ahmed, C. Birger, G.Gangl, L-E. Helander, M. Jackson, P. Krishna, R. Labiaga, C. Sayers, S. Shafer, M. Ulrich, Reader Management 1.0, EPCglobal Working Draft (May 2005)
[TDT] M. Harrison, V. Sundhar, T. Osinski, EPCglobal Tag Data Translation (TDT) 1.0, EPCglobal Working Darft (June 2005)
[EPCIS] EPCglobal, EPC Information Services (EPCIS) Version 1.0 Specification, EPCglobal Working Draft (June 2005)
[ONS] Object Naming Service (ONS) Specification Version 1.0 (October 4th 2005),
http://www.epcglobalinc.org/standards_technology/EPCglobal_Object_Naming_Service_ONS_v112-2005.pdf

Existing RFID Infrastructures
Comparison And Evaluation

Sebastian Frischbier

Databases and Distributed Systems Group
Dept. of Computer Science, TU Darmstadt, Germany

Abstract. Talking about the increase in productivity by the use of RFID technology could not easily be done without evaluating the existing commercial and non-commercial solutions. In this paper we will first define what is meant by *RFID-infrastructure* and set up some criteria for evaluating RFID-infrastructures in section two. After introducing some vendors in section three we will look at selected solutions of SAP and Oracle in detail and evaluate them with the given criteria.

1 Introduction

In context of *Radio Frequency Identification (RFID)*, the phrase *RFID infrastructure* describes the IT-infrastructure which is necessary to collect, filter and enrich raw RFID-data before processing it to the backend-systems (business intelligence systems like ERP, etc.) [1]. In our case, we are focusing on the software-components doing this job. Hence *middleware* and *infrastructure* are to be used synonymously in this paper.

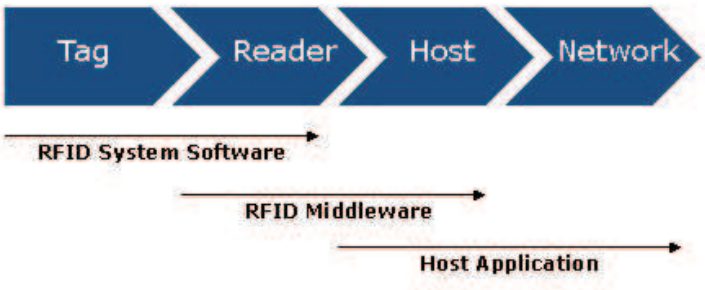

Fig. 1. Components called middleware regarding [2]

In order to standardize the technical description of each vendor's solution, we have derived a set of evaluation criteria. Furthermore we have defined three phases the act of processing RFID-data typically has to go through if working

properly. This was done by identifying and generalizing the several steps to be performed. Hence the abstract task of preprocessing data could be distinguished into three phases:

1. collecting data by managing the RFID-reader(s)
2. enriching this collected data for further use (e.g. by filtering, accumulating, etc.)
3. exchanging enriched data with backend-systems

Thus we have an n-tier design approach for RFID-middleware (usually a 3-tier-architecture presuming one layer for each phase). As further reading will show, nearly all solutions meet this approach.

2 Criteria For Evaluation

Current literature dealing with RFID-middleware offers several criteria for evaluating RFID-Systems. We have summarized the most common ones to the following topics:

Scalability An increase in throughput rates could cause the infrastructure to collapse. Being in the line of fire middleware has to offer features for dynamically balancing processing loads and handle large amounts of data and their preprocessing (like database lookups, updates, etc.) [4]. Additionally this topic covers the question of how to extend an already implemented system.

Commitment To Standards Supporting common standards simplifies upgrading, migrating and scaling of an existing infrastructure. Concerning this topic, we concentrate on the exchange of information between the enricher-layer and the backup-systems. This topic goes hand in hand with the question of application integration.

Level Of Processing And Enriching Data Besides collecting data, RFID middleware needs to filter and enrich raw RFID-data in order to transform those flows into single events. What is the level of compression (e.g. by aggregation)? Are there any possibilities to configure the subset of information needed according to the connected backend-systems (e.g. highly compressed and batched reports vs. raw data streams [1][4])? What about attaching meta-data from backend-systems or local repositories to read data?

Sharing of System Functionality In reality information has to be spread across sites, countries and even across different organizations. Thus, RFID infrastructures have to support a sharing of system functionality by their architecture. One way to accomplish this task could be a high level of modularization. Sharing of system functionality should also include the ability to share information with partners in the business process. An interesting approach for instance are the *EPC Information Services (EPC IS)* [21].

Integration Into Existing Software environments (Application Integration) RFID-middleware has to cooperate with several business intelligent systems (BI) like Warehouse-Management-Systems (WMS), Supply-Chain-Management-Systems (SCM), Enterprise-Resource-Planning-Systems (ERP) or Customer-Relationship-Management-Systems (CRM). Does each infrastructure require a specific environment to work properly? How strong are the dependencies on these environments? Are there any adapters available or have other precautions been made (e.g. by a service-oriented-architecture)? These questions may be related to the question of supported standards. Nevertheless it seems convenient to us treating them as a single item.

Customizing Possibilities to customize built-in criteria for filtering and routing data, cost of work to include customer code or third-party-modules.

3 Selection of Vendors

Concentrating on the market leaders and other strong performers seemed to be the best way of giving a representative view of today's existing solutions. Hence we tried to identify those among the large number of RFID-system-vendors. Based on [3] we narrowed the range of probable candidates by regard to the amount and quality of the available documentation as well as to single significant characteristics of each candidate. We chose the following two commercial vendors and their solutions to be introduced in detail: *SAP* and *Oracle*.

Further solutions by other vendors (e.g. Microsoft, SAVI and Sun Microsystems) as well as Open Source-approaches (e.g. Singularity, RadioActive and rfid project) will not be covered in this paper. For more detailed information about solutions by Sun we refer to [23] and [24] as well as to [25] regarding Microsoft's.

3.1 SAP

SAP offers an RFID-add-on for its business intelligence landscape which is called *SAP Auto-ID-Infrastructure (SAP AII)*. SAP was a founding member of the Auto-ID center (now called EPC Global) in 1999 and began to develop SAP Auto-ID-Infrastructure in 2001 [8]. Having compared several sources concerning SAP AII together, some contradictions emerged from the non-uniform documentation. These contradictions of theoretical approach [4] and implementation [5],[6] are illustrated in the following paragraphs.

Abstract Design We start by presenting the research-approach of an RFID-system including SAP AII as mentioned in [4]. It is designed as a 4 tier architecture which is illustrated in fig. 2:

1. *Device Layer*: RFID-readers and other input/output-devices (e.g. printers).
2. *Device Operation Layer (DOL)*: Reader-management, low-level filtering and aggregation. Consists of one or more *Device Controlers (DC)*.

3. *Business Process Bridging Layer (BPBL)* consisting of one or more *Auto-ID-Nodes (AINs), an Auto-ID-Administrator*[1] and a local Auto-ID repository which is independent from the backend-system (to store local inventory-information as well as additional master-data). This layer serves as a negotiator between the DOL and the backend-systems.
4. *Enterprise Application Layer* containing backend-systems for business intelligence (SCM, CRM, ERP, etc.). Note that they are not restricted to SAP-systems at this level.

According to [4] SAP AII consists of layers two (DOL) and three (BPBL). Comparing our abstract design scheme with AII's architecture shows that step one is translated into action by the Device Operation Layer, steps two and three by the Business Process Bridging Layer.

Device Operation Layer (DOL) As mentioned above, one or more connected DCs set up the DOL. A DC manages several readers (attached via a publish/subscribe-interface[2]). Furthermore a DC is responsible for a low-level filtering of read data, its transformation into events and handing over these events to the BPBL . The low-level filtering is done by so called *Data Processors*[3] which could be distinguished into six different types according to [4]:

1. *Filters* receive and filter incoming data according to a defined level (e.g. item-level vs. pallet-level)
2. *Enrichers* read meta data stored at the TAG-memory of the current item and add them to the event.
3. *Aggregators* bundle low-level-events to *higher-level-events* (e.g. *temperature_increased_event* [4])
4. *Writers* write new or changed data on tags.
5. *Buffers* keep temporary inventory-information (tags being in a reader's scope)
6. *Senders* transform internal events to PML/XML and send them to registered subscribers

A DC is designed to work at two modi: being at the *asynchrone listening* mode a DC *waits* for incoming events from the connected readers. The *synchrone* mode means a DC receives direct device operations (e.g. read/write-commands) from the BPBL atop and gives an immediate feedback. In sum, the *asynchrone listening* mode refers to the layer beneath, the *synchrone* mode to the layer atop. Thus, being at asynchrone mode enables to execute orders by the level atop at the same time.

[1] From now on reffered to as *Auto-ID-Cockpit (AIC)* [5][9]

[2] in this case, a DC subscribes at several readers in order to recieve RFID-data. Readers subscribe at DCs in order to be notified for updates the other way round

[3] As we will see later on, the whole DOL is treated as a third-party-component by SAP in terms of implementation

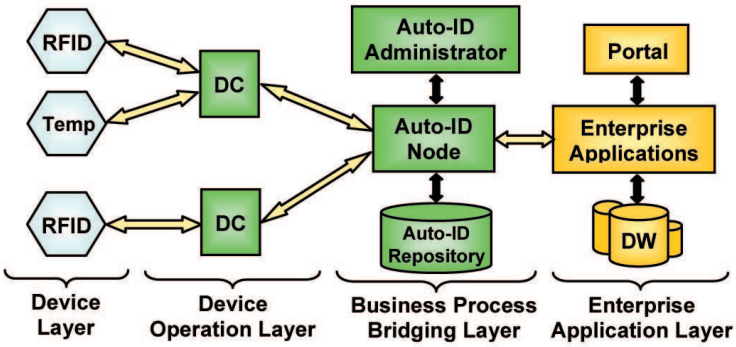

Fig. 2. figure
RFID-system as described in [4]. SAP AII-components (Device Operation Layer, Business Process Bridging Layer) are coloured green

Business Process Bridging Layer And Auto-ID Node Similar to the DOL, the BPBL consists of one or more *Auto-ID-Nodes (AIN)*. An AIN has to integrate data from several DCs into business-processes defined at the backend-systems. That means, aggregated and filtered RFID-events from the DOL have to be interpreted in terms of business-aspects in order to be suitable for the backend-systems. This is done by applying predefined rules on those incoming events. A *Rule Engine* is used to manage a hierarchical structure of those rules. One or more actions could be assigned to each one of those rules. In addition rules can trigger other rules even in other AINs. For example, reading the EPC-tag of a tracked object followed by updating the status of that object (e.g. a single item has been stored on a specific pallet, object has left warehouse) at the local repository as well as notifying the backend-systems.

Hence one could easily map business-processes to events within a AIN and thus close the gap between raw RFID-data and the underlying interpretation of that data in business-processes. Later on we will refer to these rules as *Core Services* [5] (see *Implementation* for detail). Due to that the Auto-ID Node (AIN) with its Rule Engine could be named the heart of SAP AII.

To configure and administrate the AINs and DCs, SAP offers the web-based Auto-ID Cockpit which is based on Java Dynpro [5].

Architecture What we have seen so far was a description of the abstract design of SAP AII. Now what about the implementation? We have already mentioned before, that there are some differences between theory and implemented architecture:

Comparing [4] with the description of SAP AII 2.x shows that SAP AII 2.x only consists of the BPBL with it's AINs [5][8][7]. The Device Operation Layer with its features as described above is referred to as third-party-software [8].

As a new component the SAP-Exchange Infrastructure (XI) is inserted between SAP AII and backend-systems so that there is no more direct connection (fig. 4).

Most confusing at first was a complete change in nomenclature coming from [4] to [5], [8] and [7]. Nevertheless we have tried to bridge the gap between.

According to [5] SAP AII consists only of three modules instead of AINs:

1. *Core Services* use a Rule Engine and Auto-ID-Repository to perform transformation of RFID-data to business-process-events
2. *Integration Services* encapsulate Core Services
3. *Auto-ID-Cockpit* manage Core Services and Integration Services

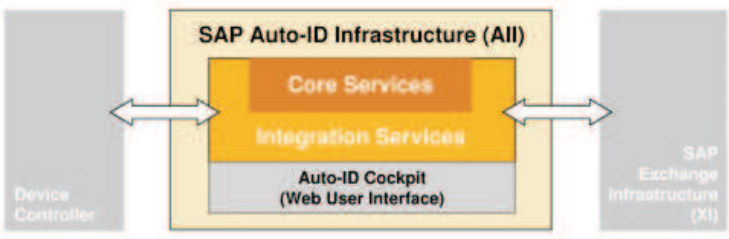

Fig. 3. figure
Core Services and Integration Services of SAP AII 2.0 taken from [5]

Core Services consist of the described Rule Engine and the assigned actions. These actions are classified according to their subject:

- *Action and Process Management:* Action Handling by Rule Engine as mentioned in *Architecture*, Event Queue, Event Message Dispatcher [Parser]),
- *Configuration and Admin Management* interfaces to devices/users, components, backend-systems
- *Object Data Management* Supervising objects (expected actions, current state, trace).
- *Lean Master Data Management* meta-data (e.g. product description) provided by backend-systems and kept at the local Auto-ID-repository.

Integration Services are used to enable interaction between AII and the following three environments:

- *Human Integration*: Administration through Auto-ID Cockpit

- *Backend System Integration*: Connection to Backend-Systems on the one hand by the use of the following two kinds of adapters: *Communication Adapters* (which provide support for several - not further documented - protocols[4]) and *Application Adapters* (to convert data directly). Provides API to access Core Services on the other hand.
- *Device Integration*: Similar to Backend System Integration (not further documented)

Although speaking of Core Services and Integration Services instead of AINs we could bring together these two nomenclatures by looking at their characteristics: Core Services consist of a Rule Engine as well as the assigned actions and are shielded to the rest of the system by the Integration Services. Hence we could define each pair of Core Services and Integration Services to form a single Auto-ID-node which could act autonomously.

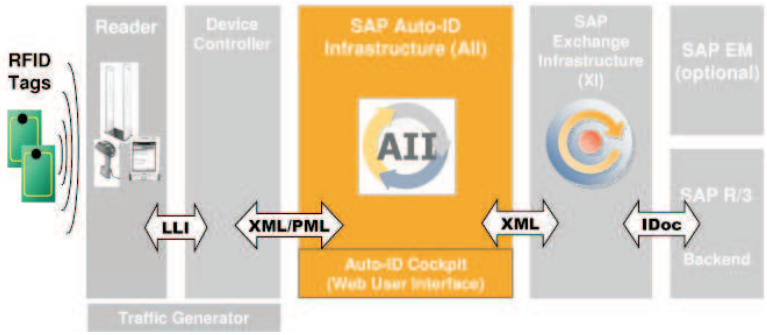

Fig. 4. figure
Scheme of an RFID-system taken from [5]. SAP AII-components are colored orange. *IDoc* is an SAP-specific XML-Format for R/3-backends

Implementation SAP AII 2.1 is designed as a NetWeaver-component and based on the *SAP WebApplication Server 6.4 (WebAS)* which contains a J2EE-application server as well as an ABAP -application server (called *Stacks*). APAB stands for Advanced Business Application Programming and is a specific 4GL programming language used by SAP. We will have a closer look at it in the following section. WebAS provides support for open internet standards (e.g. HTTP, HTTPS and SMTP) and open document standards (e.g. HTML, XML) [7]. Using the SAP-specific *Internet Communication Framework (ICF)*, programs written in ABAP can access Java or .NET-components and vice versa. In addition

[4] Supposedly XML via HTTP due to the fact that AII is based on SAP WebApplication-Server. See *Implementation* for further detail.

ABAP can process HTTP requests thus serving as a client as well as a server. At default, both stacks are installed and have their own scheme at the local Auto-ID-repository. WebAS provides *Open SQL for Java* which encapsulates the underlying databank from the developer.

SAP Exchange Infrastructure (XI) is a standalone application and has already been introduced before. It serves as an adapter between SAP AII and different backup-systems [11]. Devices from Connecterra, ACSIS and Infineon [8] are recommended by SAP to serve at the Device Layer.

Evaluation

Scalability SAP AII offers more than one possibility to scale the whole system by its architecture: Firstly, several AINs (with attached DCs) could be combined by rules at the BPBL. Secondly, several DCs could be combined at the DOL. Due to the fact that the DOL is not implemented as a part of the "core"-AII, this has to be archived by connecting several third-party-DOLs to the Core Services (by using suitable adapters). To reduce traffic to the backend-systems, a first error-handling could be performed at the AINs (Core Services respectively) by defining appropriate rules. For instance, divergencies from expected pallets (by Advanced Shipping Notification - ASN) and actually delivered ones could be recognized. A corresponding interpretation by the Rule Engine provides a more efficient way of informing the backend-system.

Commitment To Standards According to [4], SAP AII matches all standards proposed by the EPCGlobal consortium. In contrary to this statement no explicit support for *all* components of the EPCGlobal Network could be found by examining the design of SAP AII. Missing explicit support for the *EPC Discovery Services* (Object Naming Service etc.) as well as for the *EPC Information Services (EPC IS)* [21] is most striking. Nevertheless, SAP AII supports EPC-tags including support for GTIN, EPC number range and EPC-tag generation.

Concerning interfaces, SAP AII supports common standards as mentioned before: XML, PML, HTTP, HTTPS, SMTP, IDoc (an SAP-specific XML-format for R/3-backends) and J2EE (via WebAS' Java-Stack).

Level Of Processing And Enriching Data The first way to influence the level of aggregation is by configuring the Data Processors at the Device Operation Layer. Further aggregation and enrichment could be reached by a suitable configuration of the Rule Engine at the Business Process Bridging Layer. Meta-data could be attached by using the local Auto-ID-repository.

Sharing Of System-functionality As we have seen several AINs (Core Services and Integration Services) act autonomously and could be combined by the use of appropriate adapters of each node's Integration Services. Together with the Backend System Integration information could be spread through the whole system. Missing support for processing information on a global scale via EPC IS

and Discovery Services has already been mentioned in *Commitment to Standards*. Thus, SAP AII lacks of a built-in adapter to an interesting platform-independent communication-service.

Integration Into Existing Software-environments (Application Integration) In theory there are several ways to integrate AII into existing environments: By using either the NetWeaver-platform [10], the additional Exchange Infrastructure, by integrating custom adapters directly into AII or by parsing the XML-streams provided by the Integration Services. In addition one could address the ABAP-modules via SAP's *Java Connector* (for Java) or *DCOM* (for .NET) or use the underlying J2EE-application server for JMX. The cost of work to do this would be an interesting question to examine. Unfortunately we got no clue about that from the documentation available to us.

In practice one is forced either to invest in the Exchange Infrastructure or to develop appropriate adapters on his own in order to integrate SAP AII into non-SAP-environments. Thus AII has strong dependencies on surrounding SAP-systems.

Customizing The whole system (Core Services, Rule Engine, Integration Services, Devices, local repository) could be configured using the web-based Auto-ID-Cockpit. Adapters, modules and *Traffic Generators* (for testing purposes) developed by customers could be integrated using either AIC or NetWeaver.

Summary Although SAP AII was intended to be independent from the surrounding business applications the reality shows that it is still quite baked into existing SAP-structures. The most important negative aspect is that there is no explicit built-in support for common platform-independent protocols or services (e.g. SOAP) in favor of SAP's Exchange Infrastructure. Without SAP XI an integration into existing environments seems to be quite complicated as illustrated above.

Nevertheless SAP AII has two main features: The first one is the integration into NetWeaver thus admitting easy integration into systems being already managed with NetWeaver. The second one is the use of ABAP which is optimized for handling large masses of data and is independent from the underlying database by the use of OpenSQL. Rumors say that SAP stopped its equal support for AII's combination of Java- and APAB-Stack in favor of an ABAP-only version.

3.2 Oracle

Regarding RFID infrastructure, Oracle provides an out-of-the-box-solution for handling RFID-data called *Oracle Sensor Edge Server (OSES)*. OSES is a module of Oracle's more extensive framework *Oracle Sensor-Based-Services* for processing sensor-based data. Furthermore Oracle offers two software-packages: *EPC Compliance Enabler* and *RFID Pilot*. Digging deeper shows that both are just slightly more than parts of OSES reassembled to provide support for RFID-data

at a different degree. We will give a short summary of both at the end of this section.

Oracle's Sensor-Based-Services consist of the following applications:

- Oracle Database 10g (as local repository called *Data Hub*)
- Oracle Application Server 10g (to run Sensor Edge Server)
- Oracle Enterprise Manager 10g (as backend-system)
- Oracle E-Business Suite 11i (as backend-system)

In order to stress new RFID-components we focus on the Oracle Sensor Edge Server as a new component of the *Oracle Application Server 10g* and the attached *Data Hub* instead of describing all modules listed above. For further readings about Oracle's Sensor-Based-Services we refer to [14] and [15].

Architecture The Oracle Sensor Edge Server (OSES) itself consists of three layers, matching our presumptions made in the first section one-by-one:

1. *Device Driver Layer:* Management of Readers, Printers and other connected and supported Devices for input and output (e.g. RFID-label printers, light-stacks) of RFID-data.
2. *Data Processing Layer:* Cleansing and normalisation of read RFID-data, generation of events. No enrichment with meta-data at this point.
3. *Data Dispatching Layer:* Processing data to connected systems. Buffering outgoing data in an *internal queue* to prevent loss of data if a dispatcher is currently down.

All layers are managed by the *Enterprise Manager*-component. Furthermore a local repository could be applied to the OSES. It is called *Data Hub*.

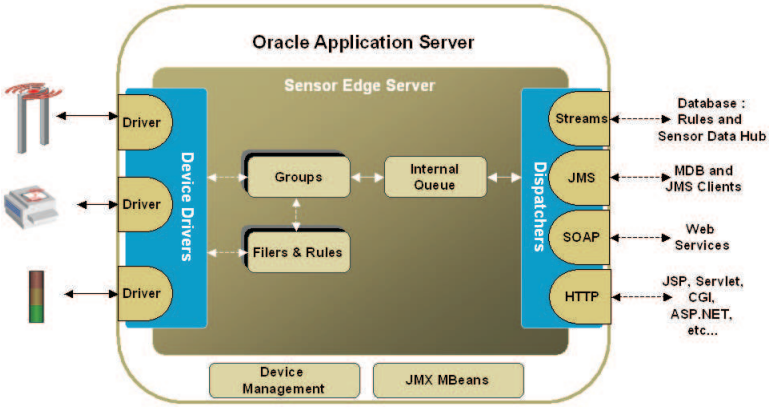

Fig. 5. Oracle Sensor Edge Server architecture according to [12]

Implementation As already mentioned, OSES is part of the Oracle Application Server 10g. Hence all advantages of this system come with OSES, too.

An important additional feature is the *Edge Developer Kit (EDK)* to develop new extensions (e.g. device drivers, adapters) and applications to be connected to OSES by unified application interfaces (called *sensor enabled applications)*. Tools for testing and simulating hard- or software (e.g. driver simulator, dispatcher simulator, reader simulator) are also included.

Each layer is designed as an open plug-in-framework with some preconfigured modules. All layers could be monitored and managed by the *Device Management*-component.

Device Driver Layer This layer is implemented as a plug-and-play-framework in order to allow the integration of new devices connected to the Edge Server. It comes with a built-in support for RFID-readers, RFID-label printers and Light Stacks. Supported Devices (in Edge Server 10.1.2) are: RFID readers by Alien, Intermec [12] and SAMSys [20], Lightstacks by Patlite and Zebra RFID-label printers.

Data Processing Layer It contains a set of mechanisms for cleaning and normalizing raw RFID-data read: Filters sweep out duplicates and aggregate single low-level-events to specific higher-level-events. Several filters are included in Edge Server 10.1.2 (see [12] for detail)[5].

- *PassThru:* Sweeps out duplicate reads of the same ID to generate a single *read* event per tag (e.g. portal readers which generate *detected*-events)
- *Shelf:* Filters data about shelfs
- *PalletPass and PalletShelf:* Aggregators for *PassThru*- and *Shelf*-events for pallets.
- *Group:* Applying filters to groups of devices (see below)
- *CheckTag:* Sort of *ping* (testing readers health).

Several devices could be grouped together via the *Groups*-component. Each one of those groups is treated as a single logical unit for filtering or dispatching. To give an example, imagine a gate with five attached RFID-readers (two at each side, one on top). To reduce duplicate reads from those readers they could be grouped together to the logical unit *NWgate*.

Regarding normalization no further information about a data-format used could be found. We assume that an XML-scheme is used here.

Data Dispatching Layer Events which have been filtered and aggregated as described above are delivered to the backend-systems by the *Data Dispatching Layer*. This layer consists of several built-in *Dispatcher Interfaces* for communication via *HTTP, SOAP, Java Message Service (JMS)* and *Oracle Streams* [17]. Again, dispatchers developed by customers could be integrated via a plug-in-framework. Thus suppliers to Wal-Mart, METRO and other vendors could integrate specific adapters to the Data Dispatching Layer.

[5] Note that Oracle includes low-level-filtering into Edge Server while SAP excludes it from AII (by defining the DOL as a third-party-component).

Data Hub And Sensor Data Rules The so called *Data Hub* is realised by an Oracle Database 10g and serves as a central data repository. It is not part of the Oracle Sensor Edge Server but closely attached to it. The main benefit of Data Hub is the use of the so called *Data Rules* which allow the definition of rules for notifications to backend-systems and the triggering of applications based on incoming events from the OSES. Hence Data Rules could be compared to SAP's *Rule Engine*.

EPC Compliance Enhancer And RFID-Pilot provide basic functionalities to work with RFID-data in EPC-format. It includes software to generate and print EPC-tags out of ASN-data. Drivers for most common RFID-readers and printers are included as well as adapters to METRO, Wal-Mart and others. Based upon the EPC Compliance Enhancer, RFID-Pilot provides further modules for prototyping and testing RFID as well as basic tools for analysis. It consists of Oracle Database 10g and Oracle Application Server 10g. To sum up, these two packages are parts of the OSES-architecture in different extent but are sold separately.

Evaluation

Scalability Since Oracle's Application Server 10g supports grid-computing [13], several Sensor Edge Servers could be combined. To have a closer look at grid computing see [16]. Regarding OSES' architecture, the *Groups*-functionality could be used to shield the real number of readers to the rest of the system. Thus, the number of attached readers could be increased or decreased at any time.

Commitment To Standards Regarding interfaces to backend-systems, OSES supports the protocols already mentioned thus offering support to the most common standards. RFID-Pilot and EPC Compliance Enabler are part of OSES so that there is an existing support for comsuming and generating EPC-tags. Unfortunately, neither EPC Discovery Services nor EPC Information Services are supported by extensions up to now.

As mentioned before, OSES provides built-in dispatchers to the most common interfaces like Web Services (SOAP), .NET, JSP, CGI, ASP (all via HTTP) and JMS as well as to Oracle-specific ones (Oracle Streams).

Level of Processing And Enriching Data The Data Processing Layer offers the possibility to control the level of aggregation by customized combination of several filters - built-in as well as those developed by customers. Hence a wide range of variation is at hand. As we have seen so far, no local repository is included directly into OSES. Attaching meta-data from backend-systems to RFID-events is still possible but requires a connected Data Hub as mentioned before. *Oracle Streams* enable the Data Hub to trigger applications written either in Java, C++ or PL/SQL upon satisfying specific rules set up at the Data Hub (compare to SAPs' Rule Engine) [17].

Sharing Of System-functionality The OSES-architecture depends on the Oracle Application Server. Thus all three layers have to be hosted by the same server. Nevertheless several servers could act as one using grid-computing, providing a share of system-functionality on this way. Regarding a share of information each OSES supports multiple platform-independent interfaces to communicate with other systems. Another way of providing a way to share information across systems could be the use of a central Data Hub.

Integration Into Existing Software-environments (Application Integration) As mentioned above the Data Dispatching Layer supports several standard interfaces and allows the integration of user-specific adapters to its framework. Thus OSES could be easily integrated even into a non-Oracle-environment just by using common standards like SOAP, JMS or .NET. The only real dependency of OSES is on an external Data Hub (idealiy a Oracle Database 10g server), provided that meta-data from backend-systems should be attached to read data.

Customization Via the included *Edge Developer Kit* drivers and adapters for new devices, services or protocols could be developed and integrated on user-side. In addition, new custom-built modules (called *extensions*) could be downloaded from [18] as well as being published there. At the Data Processing Layer, all filters could be combined (e.g. *PalletPass*). Together with the Groups-functionality the individual business-logic could be modeled using the *Device Management*. This management tool allows the administration of all three layers and is supervised itself by the *Edge Server Management*-component.

Summary Oracle's RFID-solution has two main advantages: On the one hand, OSES supports the most common interfaces as mentioned above thus reducing the need and expense of custom -built adapters in order to connect OSES to existing backend-systems. On the other hand, development and deployment of such custom-built extensions are also supported by the plug-in-framework of each layer and the public distribution of extensions over the World Wide Web.

Again, missing available support for EPC-IS and other components of the EPCGlobal network strikes as a negative aspect.

4 Conclusion

Having taken a closer look at the selected vendors' solutions they all look similar at the first view concerning design and architecture. Differences come into view when looking at the implementation due to the fact that each vendor mainly relies on one's own system (e.g. SAP favors ABAP and WebAS). Fortunately each vendor offers support for cross-platform-interfaces like J2EE or SOAP, too. The extent of support for interfaces differs very much among the vendors' solutions.

Unfortunately SAP and Oracle are not providing support for all components of the EPCGlobal Network yet. Surely this is a missed opportunity to give a positive signal towards a new cross-platform-standard to exchange RFID-data regarding their position as leaders of the market.

References

1. Floerkemeier, C., Lampe, M.: *RFI middleware design - addressing application requirements and RFID constraints*, Institute for Pervasive Computing, Departement of Computer Science, ETH Zurich, Switzerland
2. Sun: *RFID Field-Guide* - Deploying RFI - Systems. Prentice Hall, *50*
3. Leaver, S.: *Evaluating RFID Middleware - Tech Choices* Forrester Research, Inc. (13. August 2004)
4. Bornhvd, C.; Lin, T.; Haller, S.; Schaper, J.: *Integrating Automatic Data Aquisition with Business Processes - Experiences with SAP's Auto-ID Infrastructure*, Proceedings of the 30th VLDB Conference, Toronto, Canada, (2004)
5. SAP Official *SAP RFID technology - SAP Auto-ID Infrastructure 2.0 (AII)*
6. Motter, T.: *SAP Developer Network RFID Introduction.* Application Solution Management, SCM. SAP (2005)
7. *RFID-Enabled Supply Chain Execution powered by SAP NetWeaver - Using SAP Auto-ID Infrastructure 2.1.* SAP Master Guide Document Version 1.5. March 15, 2005.
8. Lemllmann, C.: *MCA202: Bringing RFID on the Fast Track.* SAP (2004)
9. SAP Draft: *Sizing the Scenario RFID-Enabled Slap &Ship Outbound Processing using SAP Auto-ID Infrastructure, Release 2.1* January 12, 2005
10. SAP Official: *SAP NetWeaver Overview* May 4th 2004 `http://www.sap.com/solutions/netweaver/index.epx` (22.02.2006)
11. SAP Official: *SAP Exchange Infrastructure* `http://www.sap.com/solutions/netweaver/pdf/BWP_SB_ExchangeInfrastructure.pdf` (22.02.2006)
12. Oracle: *Oracle Sensor Edge Server.* Oracle Data Sheet. `http://www.oracle.com/technology/products/sensor_edge_server/collateral/Oracle_SES_Datasheet.pdf` (22.02.2006)
13. Kalischnig, E.: *RFID: Making sense of sensor-based technology* in Manufacturing & Logistics, July 2004. `http://www.oracle.com/technologies/rfid/docs/Oracle_MLIT_July.pdf` (22.02.2006)
14. Klug, H.: *Entwicklung von sensorbasierten Applikationen am Beispiel des Oracle Sensor Edge Servers* in ObjektSpektrum RFID 1/05 `http://www.sigs.de/publications/os/2005/rfid/klug_OS_rfid_05.pdf` (22.02.2006)
15. Klug, H.: *Business Development Sensor-Based Services.* Sato-Symposium Hamburg 2005 `http://www.sato-deutschland.de/sato-rfid-symposium/presentations/Oracle_Holger_Klug_17.02.05%20SATO%20RFID-Symposium.pdf` (22.02.2006)
16. IDC white paper: *Oracle 10g: Putting Grids to Work* `http://www.oracle.com/technology/tech/grid/collateral/idc_oracle10g.pdf` (22.02.2006)
17. Oracle: *feature overview: Oracle Streams.* `http://www.oracle.com/technology/products/dataint/htdocs/streams_fo.html` (22.02.2006)
18. Oracle: *Available extensions for Sensor Edge Server.* `http://www.oracle.com/technology/products/iaswe/edge_server/extensions.html` (22.02.2006)
19. Oracle Sensor Edge Server Tutorial: *Getting Started - Hands on Session* `http://www.oracle.com/technology/products/sensor_edge_server/getting_started.html` (22.02.2006)
20. SAMSys Company News: *SAMSys Joins Oracle PartnerNetwork To Simplify RFID Reader Sourcing for Oracle Partners and Customers.* April 25, 2005 `http://www.samsys.com/default.php?alpha=compnews&beta=news&action=read&section=pr&release=1114446083` (22.02.2006)

21. *The EPCGlobal Network - Overview of Design, Benefits & Security*. September 24, 2004 http://www.epcglobalinc.org/news/EPCglobal_Network_Overview_10072004.pdf (22.02.2006)
22. Handelsblatt: *SAP bertriff eigene Prognose - Konzern steigert 2005 den Umsatz um 13 Prozent und lsst Konkurrenz bei Softwarelizenzen weit hinter sich*. Handelsblatt No. 8 January 11th 2006 p.11.
23. Sun Microsystems Inc.: *Sun Java System RFID Software* http://www.sun.com/software/products/rfid/index.xml (22.02.2006)
24. Sun Microsystems Inc.: *Developing Auto-ID Solutions using Sun Java System RFID Software* http://java.sun.com/developer/technicalArticles/Ecommerce/rfid/sjsrfid/RFID.html (22.02.2006)
25. Sirkaner, J.: *RFID Enabled Retail Supply Chain* http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnbda/html/RFIDRetSupChn.asp (22.02.2006)

Existing RFID Scenarios

Alex Eder, Eva Twellmeyer, and Benedict Werling

Databases and Distributed Systems Group
Dept. of Computer Science, TU Darmstadt, Germany

Abstract. The importance of Radio Frequency Identification (RFID) applications is increasing in day-to-day life. In this paper we will give a short introduction to several applications from different domains of interest. In particular we will present three topics in depth. We will start with live tracking followed by supply chain management and closing with healthcare. The topics will be evaluated regarding application examples, motives for the introduction, challenges and limits of RFID technologies.

1 Introduction

Radio Frequency Identification technology enables items, animals or persons to identify themselves by means of wireless communication. A small tag containing a microchip and antenna is applied to commercial products, animals or human beings. There are different kinds of tags which differ in shape, size, storage capability, frequency range and can be active , semi-active or passive [3]. An active chip is equipped with its own energy cell for broadcasting whereas a semi-active chip is also battery-assisted but the energy is used for the power supply of the microchip's circuitry but not for broadcasting the chips information [41]. Therefore the battery life of semi-active chips is longer compared to the life of an active chip. The passive tag on the other hand does not have a battery cell at all. It uses the power carried in the readers signal to emit its data. There are four main frequency bands commonly in use [3].

1. low frequency range (125 or 134.2 kHz)
2. high frequency range (13.56 MHz)
3. ultra high frequency range (UHF) (868 to 956 MHz)
4. microwave frequency range (2.45 GHz or 5.8 GHz)

The information stored on the tags are read by a tag reader, which induces the necessary power into the passive tags, so they can emit their data. The reader can be a handheld or a fix installed device like a walkthrough reader. It receives the identification data and supplements it with further data from local or global databases. The distance from which a tag reader can receive data from the tags can be very short (0.2 mm up to a few meters for passive tags) to a very long distance (tens of meters).

The RFID applications can be used in various fields. They can be found in baggage tracing used by airlines to reduce numbers of lost baggages. For example

Delta Airlines could decrease the number of lost baggages from usually 11 % to 0.3 % with the deployment of RFID technology [1].

Further, more access control can be realized in different ways, for exmple in ski pass, in schools, public transportation and toll system. The system for the ski pass gives automatically entry to the lift. It also helps the ski patrol to find the missing, injured or dead persons in time critical situations like avalanches. In the school the RFID chips are used to monitor attendance in school facilities and buses. Especially in Asia the tickets for using public transportation are substituted by RFID. The market leader in Asia for systems is Philips with Mifare-System. RFID is also used in toll systems to control the cars entering the highway. It is deployed in Norway and some US states.

For locating missing persons, cell phones are equipped with RFID tags, which have an additional GPRS module. RFID tags can also be found in the automobile industry and are used as an anti-theft device.

In public libraries, anti-theft devices is also an important application. As a solution all books are provided with RFID chips to protect them from unauthorized thievery. In addition these chips can be used to relieve the employees of a library, so they can focus on assisting visitors, automate the bool rental or to maintain book sorting devices and conveyer for logistic purposes [2].

In the next section, three scenarios, namely life tracking, supply chain management and healthcare, are examined in depth.

2 Live Tracking

2.1 Short history of Live Tracking and the occurring problems

The first reports, which are showing how animals were marked, are dated back to the Stone Age and early Bronze Age. Also in old Egypt reports were found, how animals were hot branded [1]. Not only hot branding was used to mark animals and prove animal ownership, but ear tags, tattoos, tail bobs and other skin altering methods were commonly used. Some animals could not be marked, because they were too small to tattoo or to attach a mark [7]. Those markings only served to prove ownership of an animal to a breeder and the marks were not recorded by a central institution. A mark and the marks owner was known only in a small region for few people. The information of the markings was spread over a region from mouth to mouth. The marking of an animal was not unique, because of the variety and similarity of the markings and marking methods. In Mexico the first central recording of marks dates back to the 16th century. There the Three Latin Crosses [18], which was used by Hernan Cortez, was recorded by a central institution. Since then the marks from other animal breeder and owner were recorded to ensure an easy way to link animals with their owner. In Spanish Texas in the 18th century the marks were kept in so called brand books, maintained by the *ayuntamientos*. Although the marks were recorded, the unique identification of a single animal was not possible. One could only identify a whole group of animals and to which breeder they belong, because the animals wore

the same marks. With registering of the marks in a central recording, the marks functionality evolved from a simple distinctive mark towards a brand. The people associated the agricultural products or animals from a certain mark owner with special properties like high quality meat or special breeding characteristics. As animal agriculture and its associated commerce have become more structured, means of identifying individual animals, not only for proving ownership, are a necessity. Today the animals are marked within 60 days after their birth with an ear tag, a ring at their foot (used with birds or very small animals), or a barcode (see fig. 1).

Fig. 1. Ear Tag with Barcode

The information of the ear tags, rings or barcodes are stored electronically or as a hard copy. The marked animals are carrying a unique number within their herd, which allows the breeder to identify a single animal. But the recording of the information is not done globally but locally for a particular breeder or for a small region. There are still enormous problems when using ear tags or rings, because the animals can easily loose their marks [4]. Another problem in tracking livestock is the long time span between birth and the marking of an animal. This makes it harder to trace an animals complete history, because the information about the animal from its first days of life can be lost. Another difficulty in this case is that the animal could have got a new identification number after loosing its ear tag and the animals first ID is unknown. While a unique identification and recording of an animals life history is an essential fact, especially in times

with many animal diseases like BSE (Bovine Spongiform Encephalopathy, mad cow disease), swine fever, avian influence and FMD (Foot-and-Mouth Disease). The arising of such diseases can upset the consumers trust in products made of animals.

Therefore a complete record of an animals history should not only raise the trust of the consumers, but it should also to help to fight against possible centers of epidemic and to get diseases as fast as possible under control [12, 13]. Also the complete history can be used to store the animals sicknesses and special characteristics of an animal for breeding purposes. Not only animals in the food industry are being tagged, also domestic animals like dogs, cats and birds are marked. Even for scientific purpose animals are tagged, so one can trace their way of wandering or the size of their territory.

2.2 Using RFID in Livestock Tracking and the resulting improvements

The RFID technology is the next step to a solution of current problems in animal identification and tracking. With the RFID tags the first steps are taken to a more transparent backtracking, covering the entire chain from the producer to the customer, and a centralized organization of animal data. The vision is that all information about an animal and the owner it belongs to, is stored in a database. Records in the database do not only consist of the information to which owner an animal belongs to, but also if an animal changes its owner, every following owner, the complete track of an animals life and disease history and which particular breeding properties it has. In Germany the "Viehverkehrsverordnung" (VVVO) guarantees that the short personal record of animals, from the birth to the butcher, is recorded. In contrast to the common identification methods used in livestock tracking, it is possible to implant the RFID tags under the skin [8] (see fig. 2), which is done near the ear or the hoof, or it can be implanted in the stomach of an animal as a so called rumen bolus.

A rumen bolus is a special RFID tag for bovine animals. An advantage of the implantation of tags is that the animals cannot loose the tag like the ear tags. So you can identify an animal and its owner at any time, as they wear the tag their whole life. Three standards apply to the tags and their technology.

The ISO-standard 11784 describes the code structure of the RFID tags. Among other things the norm contains the description of the worldwide unique, 64 bits long identification code of animals. The ISO-standard 11785 describes the technical concept of the identification chips. Further the ISO-standard 14223 applies, which describes the advanced transponder [15]. The food industry exclusively uses passive RFID tags for implantation. The tags can store the identification code as well as the tags are also capable of carrying additional information. Unlike earlier marking methods, the animals should get marked with two tags direct after their birth. The first tag is a passive tag implanted under the skin or put in the stomach, the second tag is an active tag (see fig. 3) attached to the ear. The information of the RFID tag can be read through a tag reader (see fig. 4). The reader must operate in the immediate neighborhood of the animal, since

Fig. 2. Tag implanter [19]

the range of passive tags is limited and very short. The active ear tags should make it possible to identify a single animal from a greater distance, i.e. from a car or the back of a horse.

Fig. 3. RFID ear tag (feminine part) [14]

If the animal is tagged and the owner is known, both of them are stored in a central database. The database is maintained by a private or government agency, like the HI-Tier (HI-Tier = Herkunftssicherungs- und Informationssystem fr Tiere) in Germany [16]. In addition to the stored data an animal passport (see fig. 5) is issued fot the animal, which includes the animal's ID, the owner

Fig. 4. Ear tag reader [14]

of the animal and additional information like which life form it is, which gender it has, the date of birth etc.

Fig. 5. UK animal passport [14]

If an animal is sold the information in the database is updated and the new owner of the animal is recorded in addition to the animals past owners. So you can guarantee that single animals can be tracked back to their place of origin. Even after the death of an animal the origin can be determined, because the meat of that animal carries the unique ID from the point of slaughtery to the point of sale. The database in which the collected data is stored, can be seen as a datawarehouse and a normal database. It is not only used for storing and updating the data of the animals but also for analytical purpose. The analyzed information from the database is used to breed the proper animals with particular breeding characteristics. It ensures that only animals with the best meat quality are taken. Furthermore details about special nutrition due to diseases or illnesses can also be retrieved. The information of the meat quality can only be obtained, because the meat, like mentioned above, carries the unique

ID of that animal and the food industry gives the information of the meat back to the breeder or directly to the database. But RFID technology is not only used in the food industry, but also for domestic animals. In this case the recorded information is principal used to link the pet back to its owner. The RFID technology is used as well in animal competitions like flight contests with pigeons. In this case it is used to check how long a pigeon needs for a given flight.

2.3 Problems in using RFID and possible solutions

The use of the RFID technology in livestock tracking is still not the Holy Grail for all problems, since new problems evolve which need to be solved. One of the biggest problems is the lack of standardized tags and tag readers. Some of the tag readers are only able to read the information of specific tags. The lack of standardized codes leads to big obstacles in centralizing the information about certain animals in a federal global database. Without looking at a worldwide central database, which also leads to considerably big problems. The information received from the breeder needs to be arranged, before storing it, to set them into a uniform data format. A first step to solve this problem is the standardization of the information on the tags and the standardization of the tag readers. Like mentioned above there are standards from the ISO, but another problem is that not all tag and reader producer are using the standard. Also it is not possible to ensure in all cases the uniqueness of the IDs, since they could be duplicated or in case of the loss of the tag the same number is given to more than one animal. The uniqueness can be better ensured through biometric methods, which take advantage of clear physiologic characteristics of an animal. Biometric identification methods for practical use are the DNS-Profiling, Iris-Scanning or Retina-Imaging. The DNS-Profiling is mainly used in breeding animals with best physical characteristics, but this is a very slow and expensive method, since the DNA has to be extracted and analyzed for every single animal. In the case of Iris-scanning a picture from the iris s taken and stored in a database, this method is faster and more practical than DNS-Profiling. A unique and stable mark from birth is the vessel pattern of the retina. These methods can help to make it easier to identify an animal, but the identification should not be done without tags, because the biometric methods are still under testing [9, 10, 11, 12]. Another problem is the limited range of the tag readers. To identify an animal in a herd or on an open field the breeder needs to be in the direct neighborhood of that animal. This can be solved if the animals are carrying only active tags, but it is not likely to ensure that the animals carries its unique ID its whole life, because the battery needs to be recharged. If the owner of a herd is going to identify a single animal in his herd, he will also receive the information of all the other animals, since every active ear tag is sending its information. Moreover the readers are sensitive to electro magnetic interference [5], which can falsify the broadcast information. The flood of data is not restricted to the identification of animals, but also in storing the collected data, since there were nearly 14 million bovine animals in Germany in the year 2003. Yet another problem is the security of the databases. The collected data should only be

accessible by properly chosen persons, like medical authorities to fight effectively against diseases, or the breeders themselves. Some breeders and food producers fear that public information about their herds is used for example by animal protectors or dissatisfied consumers, to weaken the trust of other people in their products, because the database contains sensitive records covering illnesses of an animal or the possible low meat quality.

3 RFID Use in Supply Chain Management

3.1 Supply Chain Management and RFID

Supply chain management aims to increase effectiveness and efficiency of entire value added chains. This means that the focus from managing a single company shifts towards managing a bundle of different companies. The challenge lies in the structure of these chains formed by the companies. Instead of having single lines with no interaction, every company has usually several different suppliers and several different customers as shown in fig. 6 which in turn makes it hard to distinguish between the chains as well as to know who is a member of the own supply chain. For example the customer in tier three might not be known in advance.

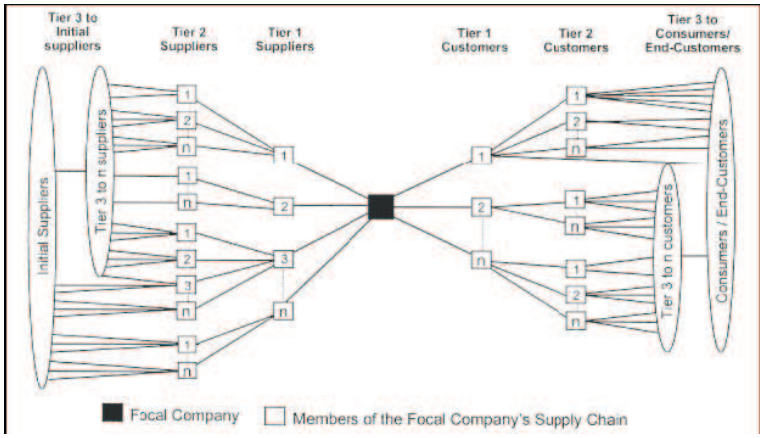

Fig. 6. Supply chain network structure [28]

Based on this prerequisite a new technology comes into place which can ease the data-exchange and provide a new quantity and quality of data regarding the different levels of the supply chain. The RFID technology has as its object to reduce or to eliminate the format discontinuity between real-life items like products on the one hand and data in IT-systems on the other hand. Fig. 7 illustrates the

gap caused by the format discontinuity concerning different methods of linking real and virtual world. The RFID technology can be seen as a mediator between the real world and the virtual world. RFID integrates the "world of things" in the system world [20]. Once the infrastructure is set up, RFID technology achieves this integration with minimal human intervention. It is capable of adjusting the system data to fit in with the real world data at a reduced cost. Furthermore RFID is able to increase the quality of the data it collects from the real world. Therefore RFID increases the integration depth by shifting the focus from e.g. a product class to the single product or from a time span to a certain point in time [20]. The availability of accurate real-time data in information systems, which in turn allows real-time management of processes, is one further characteristic advantage of RFID architectures [20].

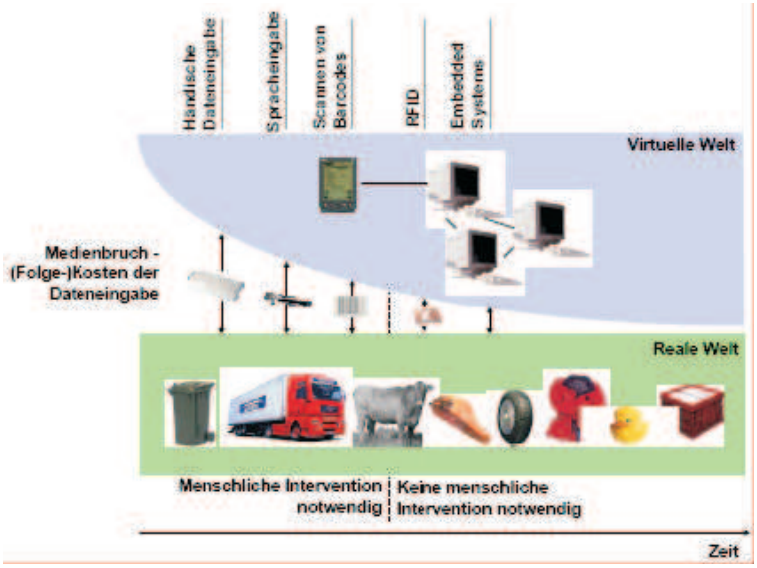

Fig. 7. Avoidance of format discontinuity [31]

Both issues, the RFID technology and the supply chain management, are about integration even though they focus on different aspects of integration. The emerging RFID technology can be applied in the also quite young environment of supply chain management. The following paragraphs try to examine the implications between the technology and the management concept.

3.2 Motives for the Introduction of the RFID Technology in Supply Chain Management

A major advantage of the RFID technology is the fact that logging the receipts of goods takes place in real-time. Therefore the inventory levels in the systems are not estimated but identical with the real world inventories. The supply chain allows exchanging this data which in turn leads to the ability to reduce inventory levels, to react faster to changing customer demand and to an increase in product availability [20]. Taking into account the entire supply chain, the bull-whip effect can be avoided, creating benefits for every member of the chain. Furthermore the processes can be controlled in real-time and process efficiency can be increased by creation of transparency. The company itself profits from reduced costs for storage and tied up capital [24]. The goal is to open up potentials for rationalization in an inter-company based value added chain. Furthermore it aims to maximize the efficiency in the overall material-flow, information-flow and in the flow of financial funds.

Another reason for the introduction of RFID labels is the possibility to trace down the product along the supply chain. This is especially important regarding food supply chains as it is also explained in part 2 live stock tracking. In the face of food scandals, avian influenza, biological-terrorism or the desire of protecting a regional brand, authorities introduce legislation making it mandatory to be able to prove the origin of a product. The EU has for example issued a decree which takes effect from 2005 on, requesting the documentation through all levels of production, processing and retailing of food [20, 21].

RFID is supposed to substitute the barcode in several areas. The advantages are information which is more precise, less missing deliveries, better traceability and an automatic identification of products which results in an efficiency increase at the point of incoming and outgoing shipments.

Fig. 8. Reading the barcode versus reading RFID labels [33]

Reading the barcode manually is more complicated, more error susceptible and more time-consuming than reading RFID-tags automatically and with no

line-of-sight. The difference can be seen in fig. 8. Therefore barcode reading does only take place at selected points in the supply chain and with a delivery just one barcode is read. Missing or wrong products inside the delivery package remain undiscovered. Furthermore, barcodes just identify the product group. RFID on the other hand allows theoretically the identification on item level. Applications like tracing down a single product, checking the best-before date or chips with sensors monitoring the cold chain are becoming feasible. Furthermore assuming tagging on item level, half of the delivery packages could be put on the shelf whereas the other half stays in storage. Still exact location data for every item is available. Analogous to todays anti-theft systems in stores, the already included RFID tag can fulfill the task as well [20, 22, 24].

Advantages can also be seen in the customer relationship management. For example in case of malfunctioning the final customer of the end-product can be identified and the product can be easily exchanged.

In addition, the use of RFID avoids shrinkage in the supply chain through administrative mistakes or fraud of suppliers, theft of employees or customers, reduction of the share of unsalable goods and it makes sure that products are at the right place, for example in a store [20].

3.3 Applications of the RFID Technology in the Area of Supply Chain Management

The use of RFID technology is profitable in industrial sectors. This sector needs very high process security due to strict regulations regarding giving evidence for information concerning the product [24].

The price of the RFID tag prevents its use on item level. Instead it started in the end of the 1990s with the deployment of RFID tags in closed logistic cycles on reusable boxes and containers. Today RFID tags are also used in open cycles as on cardboard boxes or pallets. RFID labels are still too expensive to apply them, for instance, on every single yoghurt in the super market [20]. This will become probably possible when RFID chips can be printed in mass production on polymer-basis. Already in 2003 for example it was first possible to print a transistor in mass production [25]. Even if it does not seem profitable yet to deploy RFID in the retail trade, retail companies use them on the background of intense competition and with the awareness of possible cost cuttings in logistics and on employees in stores and warehouses [24].

With the combination of the RFID technology and the supply chain management, new applications evolved. They can be divided them into problem-oriented innovations and technology-driven innovations, also called bottom-up-innovations. Problem-oriented innovations lead to process improvements carried out in small steps. An existing problem is tried to be reduced or solved using a higher quality standard when matching real world data with system data. These applications are used where current applications lack to fulfill the requirements. In the area of supply chain management these applications are control tasks for example regarding logging the receipts of goods, checking on goods, prod-

uct flows, production control, theft avoidance, damage avoidance and forgery avoidance [20].

Technology-driven innovations on the other hand start with the possibilities emerging from the new technology and are trying to find new applications which could not be controlled earlier on, for example replacement parts. The product would know by itself which ones are the right replacement parts, when parts have to be exchanged or when parts do not function properly anymore [20]. New applications like applying RFID tags instead of barcodes often need a complex infrastructure. Furthermore it is not sufficient that just one company changes its business practice. An example is a retailer who tries to build up a RFID based retail store with RFID tagged products which are read automatically when they are delivered to his store. He would probably not succeed due to the fact that most of the products will just not have a RFID chip. Therefore market players who decide to promote the introduction of a new application are usually needed. Putting their requests for the new application to their trading partners leads in a successful case to a thorough market penetration. For the use of the RFID technology in the supply chain management in the retail segment, the Metro AG is such a big player who tries to introduce the new application. Metro has designed and built a so called "Future-Store" in which customers can experience the beginning of a future grocery store. Furthermore the goods in storage are also managed by RFID chips and the technology is already being used in Metro's regular stores as well [30].

3.4 Limits and Challenges of the RFID Technology

Challenges Regarding the Use of RFID in Supply Chain Management
An important prerequisite for the wide use of RFID technology is the need for standards companies and institutions adhere to. One standard is the EPCglobal. It allows automatic identification of items and provides a supplement identification standard for the barcode in form of a numbering scheme. EPCglobal has over 400 members and is backed by large retailers and consumer product manufactures [34]. Nevertheless is the standardization process still under way and is not completed yet. This situation works at the moment because the RFID technology is not applied by the masses yet and the use normally encloses just a few partners so that own specifications can be used. Metro for example is using a centralized computer, the RFID-product-flow-system, to store all data of the RFID tags. All partners of the chain like retail stores, the centralized procurement, warehouses, wholesalers and manufacturers have access to the system [24]. Nevertheless a wide deployment of RFID needs a working infrastructure based on standards to become reality. RFID can be used in single companies, but its main improvement can be siphoned off by the use in a supply chain. The challenge is that RFID is just placing the technology at the companies' disposal. For fully unfolding its benefits a functioning supply chain and a functioning SCM are needed. Accordingly to Lambert and Cooper [28] the supply chain network framework can be divided in elements and key decisions as shown in fig. 9. The

three elements are the supply chain network structure, identifying the key supply chain members, secondly the supply chain business processes, identifying the processes which should be linked with the members and as the third element the supply chain management components identifying the level of integration for each process.

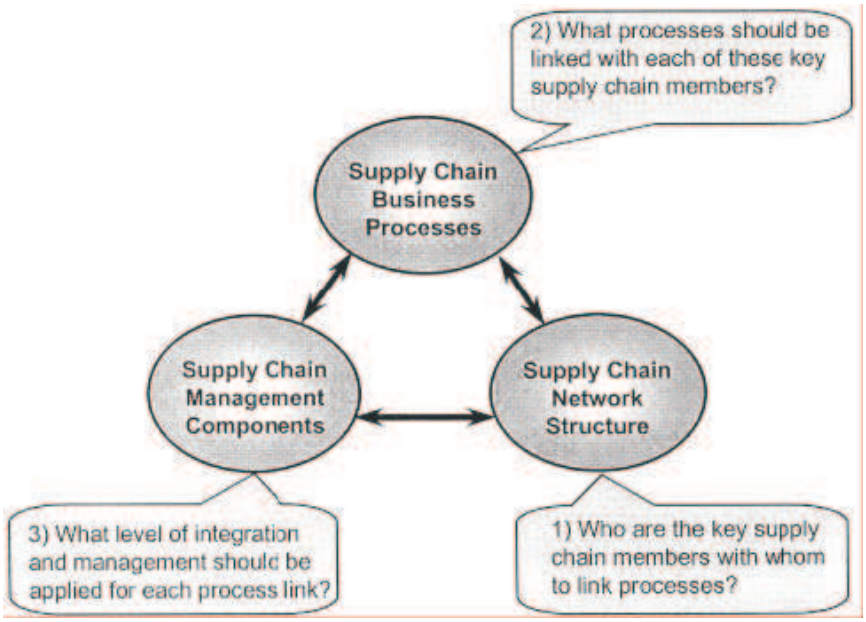

Fig. 9. Supply chain management framework: elements and key decisions [28]

Another hurdle regarding the effective use of RFID in supply chain management lies in the nature of the chain itself. Supply chain management focuses on the entire supply chain and not on one company. Therefore the objective of maximizing the value is distributed over all members. Benefits and expenses should be distributed fairly over all members of the chain so that every member aims to enhance the value and does not work contra productive. With the introduction of the new technology, RFID related costs for purchases and usage emerge which might not be distributed equally. An example are the RFID tags which have to be applied to the product in an early stage of the supply chain but deliver its value over all levels of the chain.

Additional challenges which block the wide use of RFID are the still relatively high costs for RFID tags and RFID readers [20]. So scenarios like permanently taking inventory in a store and knowing always the exact location of a product are not profitable yet. A tight net of RFID readers would be needed on the store shelves, which is still too costly to realize. Over and above RFID readers do still

lack capabilities needed for an efficient processing. For example todays readers have problems reading tags on metal and fluids or reading a great amount of tags at the same time in a small area [20].

A further barrier for RFID is the fact that RFID technology demands an integration into the company's existing software. This is the case when realizing benefits exceeding the applications which already could be realized with the help of barcodes. Additional efforts and expenses are now implied. An example is the data registration regarding individual products. Software like SAP RFID has the goal to integrate the different technologies coming along with the RFID technology. Further it aims to build an infrastructure which can manage the large amount of data, seamlessly integrate RFID into existing applications and create new applications based on the new abilities of RFID [23, 29]. Independently of SAP many IT-architectures include several layers. There are for example the transponder-level followed by the RFID-reader which passes the information on to the middleware. The middleware in turn is responsible for offering basis services like filtering and bundling up the massive amount of data as well as integrating the following complex and distributed applications like ERP or SCM. Edgeware for example is responsible for detecting and correcting reading mistakes [20, 22].

Challenges Regarding the Introduction of RFID Nowadays companies trying to introduce RFID chips in the retail segment are faced with consumer protection groups having doubts and objections concerning the customers' data protection. Also various newspaper articles covering the topic address these concerns. One example is Benetton announcing in the beginning of 2003 to include RFID tags in the cloths of its brand "Sisley". Just a few weeks later Benetton was forced to withdraw. Metro introduced a customer card with a RFID Chip, but without telling the customer. Finally Metro was also forced to withdraw its RFID-card. Similar reactions do also WalMart or Gillette encounter [20]. Some customers are afraid of the loss of their privacy sphere. This behavior stands in sharp contrast to several customers card which are successfully issued today. To achieve minimal discounts customers willingly disclose their buying patterns and allow its evaluation, analysis and interpretation. In reaction to these concerns Metro for example is offering a possibility to destroy the RFID tag after paying as shown in fig. 10 [20].

Aside from the technical implications, the customer may be satisfied at first because his privacy is preserved. But at the same time he is excluded from additional applications which might be feasible. For example the exchange of the product without a receipt.

In Germany the ministry for research and education has instructed the Unabhngiges Landeszentrum fr Datenschutz Schleswig-Holstein and the Institute for Business Computer Science of the HU Berlin to conduct a study about "Technikfolgen-Abschtzung Ubiquitres Computing und Informelle Selbstbestimmung" - anticipation of the technical implications ubiquitous computing and self-determination regarding data in the project "TAUCIS" [26]. Part of the study is

Fig. 10. device for deactivating the RFID Tag from Metro [32]

a consumer survey which should determine for example which applications the customers like to have and if they really think the car should determine when it has to check in at the garage [27]. This shows that the introduction of ubiquitous computing and RFID are not just determined by technical aspect but are also influenced by the social development due to its wide range of impact.

4 Healthcare

Large healthcare organizations are just moving faster ahead and with bigger RFID deployments compared to other industries. Jim Gallas, senior vice president of BearingPoint's health services practice, conducted in a survey that "most healthcare executives believe RFID technologies are strategic to their business in a number of important aspects, from patient safety to operational improvement. Over the next 24 months, we expect healthcare organizations will move from the strategy and pilot phases they are in today toward first-stage implementations where there will be a strong opportunity for return on investment."[37]

In the following we will examine four motives showing advantages of RFID in healthcare.

The first one is robustness. After an extensive research, very robust RFID tags have been developed. These tags survive very high temperatures. This is particularly interesting for hospital domains because they can survive sterilization. Another advantage is, that they are resistant against dirt.

The second advantage is unobtrusiveness. RFID communication is wireless, so there is no need of wires to use the RFID tags. Another advantage is that these tags can be used behind or underneath surfaces. This is one of the most important advantages, such as caring for people with early-stage Alzheimers or those with autism. In this way, it is ensured. The third one is the ease of use. With those RFID tags the patient never engages in any explicit scanning action. The convenience is also good for busy nurses or doctors. Consequently, they need just less time for the scanning process. The last is the value proposition. In the healthcare domains, cost concerns are less critical than in the supply chain industries because the system cost is often dominated by the tag costs. In this way the cost in the healthcare domain is just less as these technologies can deliver services that are so highly valued[34]. With the new technology there are accrue new costs. A new study by BearingPoint, Inc. is showing the investment for RFID technology. BearingPoint, Inc. is s a leading global management and technology consulting firm, providing strategic consulting, application services, technology solutions and managed services to Global 2000 companies and government organizations. They help customers to get access to the right information at the right time A survey of more than 300 healthcare organizations respondents in the following arguments about using or buying RFID technologies: First of all, 70 percent of respondents say that they can improve the patient security. On the second place with improved patient flow and general productivity, 48 percent consulting of these arguments and say that is very important. 30 percent of large organizations have already deployed some RFID technology, compared to

just 13 percent of smaller industries. These are big advantages about the technology, but the high costs make it hard to buy those technologies. So there are only less than 20 percent of respondents plan to spend more than $250,000 on RFID in 2006. And just more than 50 percent plan no spending at all. But in the following years more healthcare institutions plan to invest more money in RFID. With this ambition, 39 percent anticipate spending $250,000 or more in 2007 and 2008. But large organizations plan to spend between $1 million and $5 million on RFID in the years 2007 and 2008. Cost is a main barrier to adoption. More than 50 percent that it is a major hurdle to get the needed funding for the projects. And there is also another problem with the RFID technology, because 60 percent of the respondents said they have delayed some RFID activities while waiting for industry and government guidance on standards. [37]

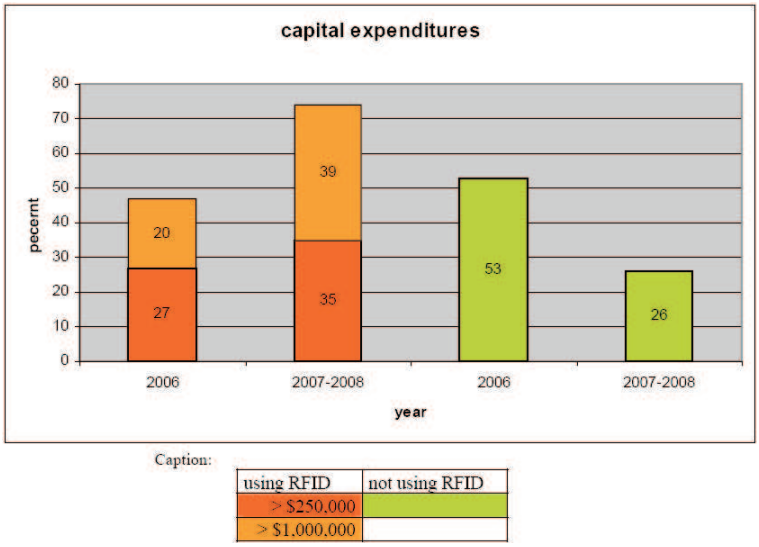

Fig. 11. Capital expenditures [3]

4.1 Applications in Hospitals

In the hospitals it is very important that people often need to be found quickly and the environment finding the right person, like a doctor or a nurse with a particular expertise or knowledge, and also a special patient, in a huge hospital can be a long journey. That can be a big problem because it is often a time-critical an urgent endeavor. At present the main application for RFID is similar to supply chain management.

The supply is defined as the doctors, nurses, patients and equipment. And the "management" consists of being able to rapidly locate them within a fixed

environment at a particular time. For example in the USA the Doctors Hospital in Dallas is partnering with Tenet Healthsystems to track newborns to ensure, they match to their own mother.

Fig. 12. Size of an implantable RFID tag [38]

There are many hospitals currently using the RFID technology for blood transfusions. The blood-handling process contains several manual steps. This way there can be a lot of mistakes, like confuse the blood container. If the patient gets the wrong blood type and as the aftereffect the wrong blood infusion can trigger reverse reaction at a person up to, and including, death. The hospitals which work with these technology systems, like the 1,100-bed San Raffaele Hospital where more than 15,000 blood transfusions are delivered each year have fewer cases of death. The systems works wirelessly. There is an RFID tag on the blood container which show the nurses if she have the right one[34].

One concern who develops those Systems is "Intel". They have developed a new RFID system for hospitals which helps the employees do their work. The new system includes:

- Better staff mobility and increased efficiency
- Improved data sharing with the hospital's back-end database
- Staff access to blood data at bedside, office, or donation area
- Drastic reduction in error potential

At present and in future it is not only new medicine which saves the peoples life of the, it is also the new technology which saves a lot of lives [35].

According to a new study by BearingPoint, Inc, the healthcare sector is enthusiastically adopting RFID technologies. Spending on RFID is set to see a rise from 2007. Morerfid.com reports: "This survey illustrates that most healthcare executives believe RFID technologies are strategic to their business in a number of important aspects, from patient safety to operational improvement," said Jim Gallas, senior vice president of BearingPoints health services practice. [36]

4.2 Safeguarding Equipment Usage

At present the RFID readers are very small. Hence, it is possible to integrate them into the hospital equipment. In particular the equipment which is dispensed or connected into it. For example as blood bags, anesthesia lines or medication boluses. With RFID it can be ensured that the correct item is connected at the

correct time for the correct patient. With this help the stress of the nurses take off and so there are less treatment errors.

RFID can also be used by pill dispensing. Missmedication is a major problem in healthcare. Every year 7,000 people die and 770,000 are injured because of that problem. With this technology the problem will be solved. In the year 2007 there should be RFID tags placed on pill bottles. If the RFID readers are placed on the repositories where the medicine is kept, the system can track whether the right medications are being taken at the right time by the right person. In a hospital the nurse can check if the person takes the right pills at the right time[34].

Fig. 13. RFID tag implantation [39]

4.3 Assisting Medical Personnel

RFID will be used as a sensor network. In this way it can display information practically, like issue reminders, notify other personnel, and so forth anticipation of the doctors needs. At present it is a long-term research agenda. The preceeding scenarios were examples of areas where it would be advantageous to have different pieces of medical equipment tagged. It is a big advantage, because you know which RFID-tagged equipment is being used when and by whom.

With those RFID-tags a computer can look at this sequence and conclude what the doctor is doing and how the doctor is doing it.

There is one project in the Anesthesiology Department of the University of Washington Medical School. At this school, the students wear a small RFID reader in a glove that fits under their existing latex glove. The glove has two antennas. The first one detects the RFID tags near the palm and the second one detects the RFID tags near the thumb.

Currently there are many questions that can be answered by looking at the RFID traces. Some of these questions are:

- Did the person use a different tool than the expert would have?
- Did they use the right tool but it took too long to use it?
- Did they waste time getting out too many supplies or, conversely, lose time because they had not done enough preparatory setup?

With the help of those RFID tags the answers can be used to improve the objectivity, efficiency, and reliability of skills assessment. It is just a checkup for the practicing people. Particularly it can save some peoples life in the hospitals because there are no longer careless nurses or doctors [34].

4.4 Home Eldercare

There are two general areas of eldercare. First, caregivers will need to keep tabs to elders. With the RFID technology the caregivers have a new security system for the healthcare about the elder people. If the old and sick persons wear those RFID tags, the caregivers have all the information about the person. So the caregivers can stay in the main office and watch the data from the people who wear one of these RFID tags. With this method they can control more people and if there is a contingency they can help faster.

The second argument for positive effect with RFID in home eldercare is that these systems can help elders with exercise, nutrition and social health. To clarify the advantage we will describe one case study about an old person and his daughter and in which way the RFID technology can help them. One old person, named Peter, is 91-year-old former teacher and lives alone in London. His daughter, named Amily, lives just one mile away. Peter is basically healthy, but he is fragile and forgetfully. So his daughter must look every day after him if he takes his medicine, makes his exercises and maintains his hygiene. This is a big problem for Amily because she must also look after her own family. A solution can be a RFID system. Now Amily is able to control her father from the distance, whether he takes his medications, looks after his hygiene, eats enough and makes his exercises. With a simple motion detector system she might be able to infer that her father gets up, moves into the bathroom and opens the medicine cabinet. The RFID tags are small enough to place them in the toothbrush or in the medicine bottles. So the system can differ whether Peter brushes his teeth or takes his medicine. The idea of this solution is that Peter also wears an unobtrusive RFID tag. He can wear a bracelet or he can have it under the skin. If Peter is using a RFID-tagged object, the reader detects it and his daughter gets the data. All the connections between the computers and RFID tags are wireless and battery-less, so there is no bothering cable. So she can be sure that he is OK. With such a system like the RFID it relieves those people like Amily and makes it for those elder people like Peter possible to live alone.

One of the problems with RFID technology, is that it very expansive at the present. For example with the Home Elder care, we will show it in a table. There

are two kinds in which way you can monitor the elder. The two systems are RFID and video. With video the caregivers can see the elderer all the time on a display. They can be sure that they OK.

Type	Cost	Privacy/Security	Accuracy
RFID	$$	High	Moderate
Video	$$$	Low	Low

Fig. 14. Analogy between three Technologies[34]

In this table you can see that the RFID technology the best in proportion to the other. The only problem is that a lot of families can't achieve the high cost. But it is a good alternative for those companies who work as carer for the elderly [34].

There are a lot of advantages about using RFID technology in home elderance. But there are also disadvantages. One for example is the cost. So for the private users it is too expansive and only rich people can use this technology to control their elder. The RFID technology is just under testing, so it is very expansive, like every other new technology. It is just impossible to use the RFID in every hospital or home elderance. The costs are too high and this is the heavyest argument that prevents the wide use of the RFID technology in healthcare. But there is also a second point showing the disadvantages of using RFID in healthcare. It is very time-consuming to install all the RFID tags in the objects in hospitals as well as in the home of elderer. In addition to the outlay a time consuming installation of the technology infrastructure is needed which in turn implies even higher costs. In the case of hospitals one can add that process changes are inevitable to adapt the environment to the new technology requesting further efforts [34].

5 "Chip, Chip, Hurra?" [40]

So entitles the German weekly newspaper "Die Zeit" in its current issue from 01/19/2006. Following the citation we will conclude whether the RFID technology keeps its promises or not.

As a concluding remark the use of RFID technology in Live Tracking is a step in the right direction. It can guarantee a consistent track of animals and furthermore a fast and effective fight against diseases and epidemics. Also logistic problems in food industry can be reduced or even solved. But the other side of the coin is that the RFID technology is still in its infancy and it will last some time until it will become widely accepted. On the one side a number of technical problems have to be solved and a common technical standard has to be created. On the other side it needs a legal basis and an adjustment of the technology to ensure data security and a smooth interaction from current technologies.

Therefore it is likely that the RFID technology becomes widely accepted, only, when the technology, standardisation and legal basis are more mature.

The use of the RFID technology in supply chain management ist still under development but it has the potential to change the way doing business among the companies involved in the chain. Introducing RFID technology is by far more complex for a company than introducing a new computer programm. It involves the use of a totally new infrastructure which often goes along with process changes. Furthermore the technology will have great impact on the end-customer and the consumer respectively who will have to face the possibility of new applications. The legal implications concerning data protections as well as the question which applications should be prohibited, which have to be accepted, which are needed and which are wanted has to be decided by society as well as how to handle these possibilities.

The result of our research is that the RFID technology is very useful in healthcare. There are many ways to make the work easier for the doctors, nurses and eldercares. So there are many controlling systems with RFID during the operations or at the nursing. This way the employees experience less stress and can work more accurately. Elder in turn have more privacy when they are supervised by RFID and know that they are fine.

RFID is just under development, but this technology has high potentials. Currently it is too expansive and it cost many time to convert the whole business. It has some problems with the security. In the opposite the technology eases the work in the industry, medical organizations or in any other businesses.

6 References

[1]. Wölk, M.: RFID-Anwendungen heute und morgen. IZT-Institut für Zukunftsstudien und Technologiebewertung. www.bsi.de
[2]. US-Fluggesellschaft will Gepck mit RFID orten. In: heise online (2004)
[3]. Wikipedia: Radio Frequency Identification. de.wikipedia.org (2006)
[4]. Biometrische Tieridentifikation. www.rifid.de (2004)
[5]. Paanovsky, G.: RFID-gesicherte Fleischqualitt. www.rifid.de (2005)
[6]. Daten die unter die Haut gehen. www.sueddeutsche.de (2004)
[7]. Daten die unter die Haut gehen www.sueddeutsche.de (2004)
[8]. Elektronische Tiermarkierung. www.virbac.at
[9]. Biometrie fr's Schlachtvieh.
[10]. Biometrie fr's Schlachtvieh. www.handelsblatt.com
[11]. Biometrie fr's Schlachtvieh. www.handelsblatt.com [12]. Nutzen von RFID? Der Beweis lebt www.ecin.de (2005)
[13]. Panovsky, G.: RFID kommt auf das Rindvieh. www.pressetext.at (2005)
[14]. Dalton IDSystems. www.dalton.at
[15]. ISO 11784 / 11785 / 14423. en.wikipedia.org
[16]. Picture Barcodes: Sina Eetezadi; Ausarbeitung RFID: sina.eetezadi.de
[17]. British Cattle Movement Service: Cattle Tracing Guidance Notes and Cattle Passports. www.defra.gov.uk (2002)

[18]. Four-thousand-years and counting: the branding fire still burns ; www.farmandranchguide.com
[19]. Tag Implanter. www.biomark.com
[20]. Fleisch, E., Mattern, F. (Hrsg.): Das Internet der Dinge: Ubiquitous Computig und RFID in der Praxis.Springer-Verlag Berlin Heidelberg (2005)
[21]. Ein RFID-Chip auf jedem Apfel. In: heise online. www.heise.de (2005)
[22]. BITCOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.: White Paper RFID Technologien, Systeme und Anwendungen. (2005)
[23]. RFID-enabled Supply Chain Execution. In: SAP Solution Brief. www.sap.com (2004)
[24]. Bundesamt fr Sicherheit in der Informationstechnik: Risiken und Chancen des Einsatzes von RFID-Systemen. www.bsi.de (2004)
[25]. Forschungsgesellschaft Druckmaschinen e.V. Gemeinsam mit dem Verein Deutscher Druckingenieure e.V.: 50 Jahre Gemeinschaftsforschung und Druckingenieure. Frankfurt (2005)
[26]. Technikfolgen-Abschtzung Ubiquitres Computing und Informationelle Selbstbestimmung. TAUCIS. www.datenschutzzentrum.de
[27]. Lütge, G., Spiekermann, S.: Soll das Auto die Wekstatt alarmieren? In: Die Zeit Nr. 45, Zeitverlag Gerd Bucerius GmbH & Co. KG (2005)
[28]. Lambert, D. M., Cooper, M. C.: Issues in Supply Chain Management. In: Industrial Marketing Management 29. Elsevier Science Inc. (2000)
[29]. RFID Technology: Changing Business Dramatically, Today and Tomorrow. In: SAP Solution in Detail. www.sap.com (2005)
[30]. Wolfram, G.: Der Einsatz von RFID in der METRO Group. SATO RFID-Symposium (2005)
[31]. Fleisch, E., Mattern, F., Billinger, S.: Betriebswirtschaftliche Applikationen des Ubiquitous Computing Beispiele, Bausteine und Nutzenpotentiale. www.vs.inf.ethz.ch (2003)
[32]. Metro Group Future Store Initiative: Die Metro Group und RFID Informationen zur neuen Technologie im Handel (2005)
[33]. Wlk, M.: RFID-Anwendungen heute und morgen. IZT Institut fr Zukunftsstudien und Technologiebewertung. www.bsi.de (2004)
[34]. Garfinkel, S., Rosenberg, B.: RFID Applications, Security, and Privacy, Addison-Wesley (2006)
[35]. Using RFID Technologies to Reduce Blood Transfusion Errors. www.intel.com (20.01.2006)
[36]. RFID in Healthcare. www.rfidgazette.org (20.01.2006)
[37]. Large Healthcare Organisations Are Embracing RFID. finanzen.net (2005)
[38]. RFID Tags & Implanters. www.biomark.com
[39]. DIY RFID Implant. www.coolorwhat.net (2005)
[40]. Hamann, G.: Chip, Chip, Hurra? www.zeit.de (2006)
[41]. RFID Journal: GLOSSARY OF RFID TERMS. www.rfidjournal.com

Privacy and Security in RFID Systems

Architectural Considerations to Protect Privacy and Enhance Security

Marcel Queisser and Florian Dautermann

Databases and Distributed Systems Group
Dept. of Computer Science, TU Darmstadt, Germany

Abstract. Due to the improved production methods of microchips their prices fell, resulting in the possibility to start mass production of RFID tags. This created an interest in RFID systems from industry and commerce. These devices were deployed for security and monitoring issues and raised public concerns regarding violation of privacy and information security. These concerns are partly legitimate and must be taken seriously, others are simply caused by the fear of the unknown or by 'big brother scenarios' published by RFID opponents, which are technically impossible with the RFID tags of our time or the near future.
In the following paper we will discuss security and privacy issues raised by increasing usage of RFID systems. First we will give a summary of the design principles of an RFID system and some usage scenarios. Afterwards we will have a look at architectural methods, describe them and analyze them with respect to their grade of security and/or privacy. Finally, we will provide a perspective of the problems to be solved and what could be addressed in future research.

1 Architecture

The RFID technology itself consists of three elements: RFID tags, RFID readers and possibly a computer network that is used to connect the readers.

The tags consist of an antenna and a silicon chip that contains a receiver, a modulator, control logic, memory and a power system. Depending on how the system is powered, they are labeled as passive, semi-passive or active tags:

- **Passive Tags:** Passive tags are small and cheap. They use the energy of the reader to respond which makes them readable over decades but results in a short reading range and bad reliability.
- **Active Tags:** Active tags have a power source of their own, which results in larger reading range and good reliability. Their lifetime is limited by the lifetime of the power source.
- **Semi-Passive Tags:** Semi-passive tags which have a battery but use the power of the reader to transmit messages. This results in good reliability but limited range.

Another criterion for categorizing RFID tags is how they respond to readers. A tag that communicates with every reader is called promiscuous and one that needs some kind of authenticating, e.g. via password, is called secure.

Like other technology RFID systems can be divided into different layers. According to [7] there are three layers as shown in Figure 1:

- **Application Layer:** the application layer deals with user-defined information, e.g. information about the tagged object or an (unique) identifier.
- **Communication Layer:** the communication layer specifies how reader and tag communicate. Identifiers to isolate a specific tag are found here, just as collision avoidance protocols.
- **Physical Layer:** the physical layer defines the physical rules for the communication, such as frequency, data encoding, modulation etc.

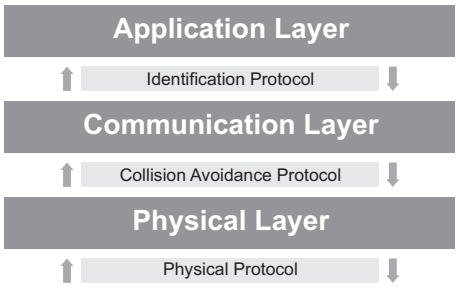

Fig. 1. RFID-Layers [7]

RFID readers send a pulse of radio energy to the tag and listen for its response. The first readers could only read one particular kind of tag but are continuously replaced by so-called multimode readers that can read many different kinds of tags.

The RFID physical layer consists of two elements, the antenna and the radio. The radio band (a specific part of the frequency spectrum), in which the tag operates, differs according to its use and the region it is used in (cp Table 2). The amount of radio energy an RFID system can collect and transmit depends on the size of the antenna. By using larger antennas, both the efficiency and reliability can be increased.

2 Scenarios

RFID systems can be used in various scenarios. Generally RFID tags just transmit a number of a certain length. How this number is interpreted depends on the network the reader is connected to. One of these networks consists of the Electronic Product Code (EPC) and the Object Name Service (ONS). These

systems are intended to be used in supply chain management. The EPC is designed to give every manufactured item a unique ID throughout its life cycle. The used tags are usually promiscuous. The ONS is very similar to the DNS. It is a distributed database which decodes the different parts of the number. Typically it is a 96-bit integer, which contains the product serial number, a number for identification of the manufacturer and the factory the item was built in. It also identifies the unique item itself and the market it is intended to be sold on. This means that supply chain management could become far more transparent and the exact inventory of a store could be known, making it easy to determine when a specific product has to be ordered. Due to problems of readers interfering with each other, the cost of the tags and problems of reading each item on pallet due to water or metal inside the package, which interfere with the energy of the radio signal or even alter it, RFID tags are only used to identify the packages for distribution and not to identify every single item in a specific package yet.

Another possible use of RFID technology has increased public interest in security and privacy issues. Implantable chips can be used to track and identify animals and human beings. Initially intended for usage in the medical field, e.g. for identifying Alzheimer patients or tracking patients and medical records, there are systems which can be used to monitor the position of the wearer via GPS.

Considering security, RFID systems can be used as part of access control systems. For these applications it is possible to combine different identification methods like retinal scans or fingerprints with the unique number of an RFID tag to grant or refuse entry or access, thus creating a higher level of secureness.

Given these usage scenarios there is an increasing demand for mechanisms to ensure security and privacy. The most important issue for the private sector might be traceability whereas the commercial users of RFID systems want their data to be secured against competitive intelligence. Different approaches like 'killing' of tags are already implemented but other techniques are considered and will be discussed later on.

3 Security Mechanisms

There are two main security problems in RFID systems [6]. The first is about attacks which try to prevent the system from functioning by means of denial of service attacks or something alike. One can do very little against this problem, because if someone jams the specific radio band no communication is possible and the only possible action against this is to find the jamming device and deactivate it. The second problem is information leakage, i.e. the tag telling the attacker something about the tagged item. Information leakage can be avoided by sending an identifier which has nothing to do with the item. The attacker has then to contact the database to determine which item it is, but the database will reject his request because he will not be able to authenticate himself as an authorized reader.

In order to gain non-traceability, the identifier has to be different in each questioning. This can be achieved by different methods, which are discussed in Section 4.

In this chapter we will discuss different means of tag/reader authentication, which is in fact the main security task concerning RFID. In our paper, we will regard a secure RFID system as *a system, in which only authenticated readers can access the tag's data (either directly from the tag or from a database using the tag's identifier).*

3.1 MAC Implementation

MACs (Message Authentication Codes) are one yet very simple approach for secure identification of RFID tags [19]. Each of the so called μ-chips (MAC-equipped RFID chips) have a 128 bit ID which is permanently stored on the chip at manufacturing time. This ID consists of an encrypted MAC and the chip data. The MAC is created by taking a part (or all) of the chip data applying a hash function and an encryption with a secret key. This secret key is known to the manufacturer and the clients. The main benefit of this method is a heightened difficulty for the creation of fake tags and eavesdropping. Privacy is not provided due to the fact that the μ-chip always sends the same ID, so an attacker could compare the IDs and track the chip. Also there is a high chance of the key being compromised due to many devices, people and/or institutions knowing the key.

3.2 PUF Circuits

During the fabrication of ICs (integrated circuits) there are minor variations which lead to individual characteristics of each IC [19]. ICs which differ from the standard can be used as so-called PUF (Physical Unclonable Functions) circuits. Different PUF circuits do not react in the same way to given challenges. Some hundred of these PUF circuits seem to be enough to distinguish 10^9 chips with a probability $p \approx 1$ to 5×10^{10} by using 800 challenge response pairs.

This can be used to authenticate RFID chips. A reader questions the tag with a set of some hundred challenges and the tag evaluates these challenges with its PUF circuits. With this method, a unique response is generated and the reader can question the database to identify the tag. A big problem for this is a replay attack, where the attacker records the challenge answers and builds chips, which behave like the PUF circuit equipped chip to this specific challenge set. To counteract that, a list of possible challenges can be used or encrypted communication can be used to deliver the challenges and the responses.

The PUF circuits function as a hardware decoded secret key for the RFID tag. As long as an attacker cannot replicate a PUF circuit or is able to model the behavior of the PUF circuit, this system is safe. Due to these tasks being difficult ones, the PUF circuit based security is a promising field of research.

3.3 Shared Secrets

Another authentication scheme is the Shared Secrets scheme [19]. In this scheme, the reader receives a tag's label and two timestamps associated with the label (T_{old} and T_{new}). The reader then contacts the tag distributor on a secure channel. The distributors database then supplies the reader with a label secret K and a cyclic redundancy check performed on the Key (KCRC). Afterwards the reader generates a random number and performs an exclusive or operation on the KCRC and the random number (RN1r). It then sends the RN1r and the KCRC to the tag and the tag obtains the RN1r. The tag now generates a CRC on the RN1r (RNCRC) and transmits it back to the reader. By this, the reader verifies that the tag is authentic. A schematic illustration is given Figure 2.

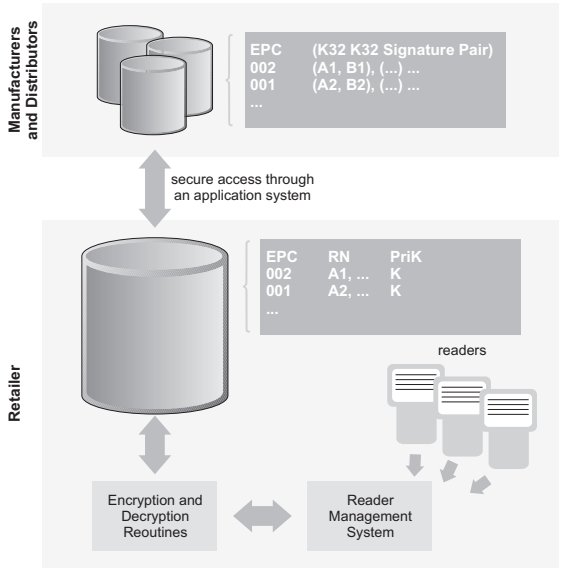

Fig. 2. Authentication Using a 2 Shared Secret Scheme [19]

Now the tag needs to authenticate the reader and therefore the reader performs an exclusive or operation with the label timestamps T_{old} and T_{new}. The chip then tests if T_{old} matches to its timestamp and, if positive, stores T_{new}. It will then wait for the reader to send K and Rnr1 after an exclusive or operation. After verifying that the reader did send the key stored in the memory of the chip, it grants the right of manipulating its resources to the reader.

Alternatively, two secrets A and B can be used, but for this method, the chip has to be able to generate a random number. The key B is then used by the chip with a random number of its own and the reader compares the obtained value B with the corresponding value he gets from the database.

3.4 Many Shared Secrets

Another method of authentication especially for chips with a small memory and/or poor processing power the many shared secrets scheme [19]. In this scheme, several random numbers, which function as authentication keys, are stored in the tag. A reader now reads the label of the tag and obtains the information which database to contact. The database tells the reader, after the reader authenticated successfully, the next authentication code, which is then transmitted to the tag. The tag compares the obtained value with the next value in its memory. It then responds with a corresponding authentication code which is only known to the database and the reader verifies this code. Both the database and the tag now increment a counter to define the next authentication code. The tag and the reader are now authenticated.

The number of these authentication codes is limited, so they represent the number of times, a tag can be read. This technique is unsusceptible to eavesdropping, because it uses different authentication codes each time, so a replay attack is not possible. Yet, a physical attack is still possible but it is not possible to produce many fake tags with this information, because each authentication code can only be used once and they have to be used in the right order.

3.5 Distance Bounding

RFID systems can be used to provide services specific to the user's context or location. To ensure that the position of a mobile device is within the proper bounds and thus prohibiting location spoofing, secure distance-bounding protocols must be implemented to enhance traditional authentication methods, which are described in Sections 3.2, 3.3 and 3.4. A way to implement such a protocol is shown in [12]. In the context of building access control using RFID, a main threat are relay attacks. In a relay attack an attacker uses transponders to relay the information exchanged by the reader and the tag over a larger distance. Proxy devices are placed near the token and the reader. The proxy reader powers up the token and the proxy token establishes contact with the reader. Both proxy devices forward any received data. This results in the actual reader reporting that it has verified the presence of a token. In order to prevent these spoofing attacks a secure-positioning protocol must be integrated into the physical layer of the communication protocol.

The distance and the delay between two stations can be calculated using (1) and (2) where c is the propagation speed, t_p is the one-way propagation time, t_d is the processing delay of the device and t_m is the measured total round-trip delay.

$$d = c \cdot \frac{t_m - t_d}{2} \tag{1}$$

$$t_m = 2 \cdot t_p + t_d \tag{2}$$

With these values measured by several base stations the position of a device can be obtained using triangulation. The protocol described in [12] defines two

actors, the verifier V (the RFID reader) and the prover P (the RFID tag), which interact in a challenge and response technique. At the start V sends a nonce N_V, which consists of a unique unpredictable bitstring, to P. Both use a previously defined pseudo random function h and a secret key K to calculate two n-bit sequences R^0 and R^1:

$$R_1^0 R_1^0 R_2^0 R_3^0 ... R_n^0 || R_1^1 R_1^1 R_2^1 R_3^1 ... R_n^1 := h(K, N_V) \tag{3}$$

After a predefined number of clock cycles a sequence of challenge-response exchanges starts. V generates an unpredictable challenge bit C_i which is replied instantly by P with a 1-bit response R_i^0 or R_i^1, depending on the value of C_i. If the response time does not exceed a sufficiently short time t_m for all $1 \leq i \leq n$, V is satisfied that P is not further away than d.

The cryptographic function h can be calculated before the challenge-response phase begins, thus removing the time factor. During the protocol, P will only reveal half of the calculated values calculated by h. An attacker could accelerate the clock-signal of P and transmit a guessed challenge $C_i^{'}$ which is correct with a probability of $\frac{1}{2}$. He can now obtain the correct response to the challenge in advance. If $C_i^{'}$ was wrong, the attacker can guess the right response with a probability of $\frac{1}{2}$. This results in a probability of $\frac{3}{4}$ for the attacker to reply correctly to the challenge. Considering n challenges, the probability of answering all correctly is $(\frac{3}{4})^n$.

3.6 Zero-Knowledge Tags

Another approach to tag security is using a zero-knowledge protocol to verify that a reader is authorized to read a tag [14]. During the authentication process no information about the tag is revealed. Furthermore after authentication the retailer can put the tag into privacy mode. In privacy mode the EPC of the tag will be deleted and transmitted to a portable RFID reader along with a shared secret device key. With this key it is possible to communicate with the tag using the zero-knowledge protocol and restore the EPC.

3.7 Noisy Tag

Some of the above implementations/protocols are based on the fact that the reader and the tag share a common (session) secret key. But in many applications this is not the case. Out of this, the need for a key exchange protocol arises. We will briefly describe NTP, a key exchange protocol proposed by Castellucia and Avoine in [8].

In this technique, the reader broadcasts random bits, noise N(i). The tag sends the secret Key bits k(i) over the channel on the same time. An eavesdropper now hears s(i) = k(i) + N(i) which gives him no information about the key. The reader on the other hand can subtract the noise and obtain the key k(i). The key is then exchanged and a secure communication can begin. In [8], two protocols

which use this technique are specified, one bit-based protocol and one code-based protocol. [8] also gives two application scenarios, the much talked about e-passports, which carry very sensitive data and therefore have to be strongly protected, and Libraries, whose books' tag identifiers need to be freshly generated each time it is borrowed to prevent privacy invasions. The authentication process is not part of NTP, this has to be done by other means.

3.8 Trusted Computing

Changing the design of readers with techniques from trusted computing can improve the security of RFID systems by introducing a Trusted Platform Module (TPM) to the reader, which ensures security and privacy of communication even if the reader itself gets compromised [18]. The design for a trusted reader consists of three parts which are illustrated in Figure 3:

- **Reader Core:** The Reader Core contains all parts of the basic functionality of the RFID reader. It has an interface which connects it to the TPM. All application run on the reader cannot modify the Reader Core and the TMP is not compromised by the Reader Core. A trusted process runs as part of it and monitors everything that is launched. The business logic of the RFID reader is not part of the Reader Core so it can be updated, if the privacy properties can be guaranteed after the update.
- **Policy Engine:** The Policy Engine is a software module which contains a policy file and controls tag-reader secrets. The policy file grants the reader permission to scan tags and determines the possibilities of the use of the data. If the reader needs a secret to decrypt information obtained by reading a tag the Policy Engine provides the secret.
- **Consumer Agent:** The Consumer Agent (CA) logs every reading operation and whether it has been performed or denied. The reading log and the policy details can then be transmitted to a controlling organization at regular intervals or on demand. The CA also reports if the configuration of the system gets compromised. Another benefit of using remote attestation is that the owner of the reader can verify that a particular CA is running. The automated sending of policy details and the ability to check the running CA ensures that the CA is mutually acceptable to both the controlling organization and the owner of the reader.

4 Privacy Mechanisms

Unfortunately, the long-term security of label contents cannot be guaranteed even if the antenna is destroyed. Then the chip's data can not be accessed wirelessly but it can be accessed by physical means, so long-term secrets, such as secret keys, are not stored on RFID labels [19]. It would be foolish to store a fingerprint on a tag, because a fingerprint can not be changed if it is lost. But it

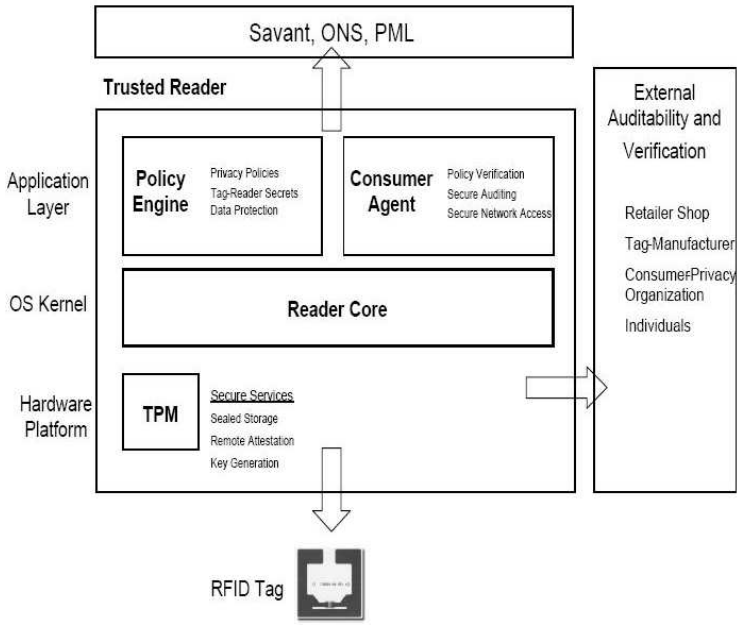

Fig. 3. Block Diagram for a Trusted Reader [18]

would be efficient to store the fingerprint in a database. If the key is compromised the database can prevent further access with this key.

Privacy can be realized by different means [7]. The simplest approach is to kill the tag, i.e. making the tag unreadable by detaching the antenna or by other means. This is a very good protection for the privacy of the tag owner but the tag is then unusable. A softer method is the shielding of the tag from the reader, so the tag can not hear the request by the reader. This method is suitable only for some scenarios, e.g. special shielded wallets for tagged money, tagged credit cards, etc. (an instruction to construct such a wallet by simple means can be found in [9]). Another thing one can do to protect ones privacy is to carry a so called blocker tag. It is an active tag which broadcasts random numbers on the radio band, thus preventing any other tag reading. This is again a very efficient privacy mechanism but it makes using RFID benefits harder and this method requires a lot of energy. The most promising, but yet sparsely researched, techniques are protocols which restrict the access to the content of the tag. Some of these techniques will be described later in this chapter.

In our paper, we will regard a privacy protecting RFID system as either *a system, in which only authenticated readers can link two sightings of the same tag (software privacy protection)* or as *a system, in which reading the tag is (temporarily) prevented by physical means (hardware privacy protection).*

In contrast to security issues, it is not sufficient to guarantee privacy, i.e. in fact non-traceability, on the application layer. It must be ensured on all three layers.

- **Application Layer:** to ensure non-traceability, the tag has to provide different messages each time it is questioned. The reader has to understand these different messages but for an attacker they have to look like random numbers. Either the tag can generate a new number of its own, e.g. by applying a hash function (this method is secure but hardly scalable), or the reader gives the new value to the tag. In this case, the messages to the tag may only be used once and they have to look like random numbers to the attacker. This is a difficult goal, which unfortunately not all protocols achieve.
- **Communication Layer:** the most important challenge for the communication layer is the singulation with collision avoidance mechanisms. Singulation is needed to guarantee the undisturbed communication between a reader and many tags in its proximity. The reader and the tags agree on dividing the radio band by means of time division. These singulation methods can be either deterministic or probabilistic. Most deterministic approaches use a tree walk algorithm, in which the reader questions increasing prefixes of the identifiers until only one tag responds. This is a security risk, because a tag could be traced in an uncompleted singulation session (because the identifier cannot be changed during a singulation process).
  Most probabilistic approaches are based on a slotted variant of the Aloha protocol. In this method, the reader tells the surrounding tags to answer in n defined slots. If a collision in slot x appears, the reader questions the tags to retransmit if they transmitted in slot x before. An attacker could question a single tag, save the slot x in which the tag answered and then follow this tag by always telling it, that there was a collision in slot x (the reader has to store the new slot after each interrogation). Another tag will only respond if it is also in an uncompleted singulation session and did transmit in slot x in the previous round, which is highly unlikely.
  A timeout, which aborts the singulation process after an unusual long time could solve these problems. Another problem discussed in [7] is the lack of randomness, caused by poor random number generators in the tag and/or bad protocol specifications, which results in traceability of the tags.
- **Physical Layer:** due to different standards for the communication between the tag and the reader, it could be possible to track a person by following his/her characteristic mix of standards. Another problem on the physical layer is the radio fingerprinting. Each type of tag behaves a little bit different while sending and this is called its fingerprint. So, an attacker could follow a specific tag or again a specific mix of tags with a high probability.

4.1 Erasing the EPC

Tag owners can be tracked by comparing scanned EPCs [19]. This can be avoided by simply 'killing' the tag, which means destroying the tag by disconnecting the

antenna and/or destroying the rectification circuit. This removes all privacy concerns but prevents many benefits for the customer [14]. Another possibility is to recode the tag with the original EPC shortened to the product information thus preventing the unique identification. However, it is still possible to violate the privacy by examining the types of products someone carries.

4.2 Recoding

It is possible that RFID tags can be used for competitive intelligence [21]. Considering tags without proper authentication protocols it would be easy to monitor the shelves of a store by simply walking through it with a reader hidden in a backpack. There are two possible solutions. The first and easiest solution requires to kill all tags, as described in Section 4.1, before placing the tagged items on the shelves. This solution prevents the usage of all other benefits, like monitoring the inventory of the store. Another solution is to use store-specific tag IDs, which cannot be understood without knowledge of the internal information systems of the store. This could be achieved by recoding the EPC with an internal code.

4.3 Re-encryption of Tags

As explained in Section 1, RFID tags with an EPC usually respond to questioning readers by sending their EPC without verifying the authorization of the reader. This imposes a threat to security and privacy, so it is crucial to control access to the tags EPC or to allow the reader to respond to the questioning with a response that does not contain the EPC. One possibility for this is re-encryption [19]. This technique requires at least class 2 tags (cp Table 1)), because their content must be rewritable. The retailer concatenates the EPC with a random number, encrypts the result and stores it on the tag. The key to this encryption is only known to the retailer. When requested, the tag sends the encrypted data, which will appear as random numbers to an attacker. An authorized RFID reader can decrypt the message and receives the original EPC and the random number. Then, it can rewrite the EPC on the tag, again padded with a random number and encrypted with a key. And even the customer can reencrypt the EPC with its own key, so only he and authorized persons can access the EPC. With this technique, the end user has all the benefits of having unique EPCs on his tagged items without the privacy issues occurring with promiscuous tags.

4.4 Pseudonym Protocol

The two main problems concerning privacy are the linking of two sightings of a tag and ownership transfer, where only the new owner should be able to read the tag. These problems could be solved by a protocol proposed by Molnar, Soppera and Wagner in [17], which we will describe in this section.

What is new in this protocol is the delegation. A tag generates a pseudonym ID code with its secret key and sends this ID code, which a normal reader (a

reader which is not generally allowed to access this specific tag and therefore does not own the secret key) does not understand. The reader passes this ID code to the appropriate trusted center which gives information about the real ID of the tag to the reader if it can authorize itself by well-established cryptographic means towards the trusted center. The trusted center has been given all relevant data about the tag, i.e. the secret key, the ID code, access policies etc., on the rollout of the tag. An authorized reader is able to decipher the real ID code by himself. With two responds of a specific tag being never the same, the problem of traceability is solved, because an attacker can not link two sightings of the same tag.

The concept which is used here is called *Controlled Delegation* which means, that the trusted center decides whether it gives the information to the reader or not. It is important that the trusted center does not give the key to the reader because then the reader would be able to read the tag for all time, which also opens the door for physical attacks on the readers memory to get the key. So the trusted center deciphers the ID and passes it on to the reader. The next time the reader sees the tag, it will not recognize the tag as the one read before.

But also, if the reader should be able to read the tag for a limited number of times, this is possible. Therefore, the trusted center gives the real ID of the tag and the next n pseudonym IDs the tag will respond, where n is the number of times the tag should be readable by this reader.

Ownership transfer is also made secure with this technique. When a tag changes hands, the trusted center simply does not grant access to the old owner anymore and grants access to the new owner.

A method to improve scalability and enhance the delegation between different trust center entities and/or readers, i.e. giving secrets to enable a permanent readability, can also be found in [17].

4.5 Privacy-Protecting Tag

A simple way to protect the privacy of tag owners is to reduce the size of the antenna, thus reducing the read range of a tag. It would still be readable and fully functional, but the reader would have to be significantly nearer to the tag. IBM proposed such an architecture of tags with alterable antenna size [15]. This altering could be done by scratching off printed conduit that links two parts of the antenna or by stripping off a part of the antenna at a built-in perforation line. With this method, the read range can be reduced from a few meters down to 2.5 to 5 centimeters. Even with highly amplified readers, the read range would not exceed about 15 centimeters according to estimations by IBM. This is a significant improvement to consumer privacy because one can control the readability of the tags easily by not letting a reading device come very close to the tag but the tag can still be used for applications useful for the consumer.

5 Perspective

RFID is a very active field of research which has to deal with several problems as we have shown. New protocols are implemented and are poorly checked if they are secure against attacks and/or privacy assaults. Only few standards are yet established; different research groups come up with many new ideas. The EPC of the Auto ID Center as described in Section 2 and in [10] (chapter 3) is a positive example for the standardization of RFID technology. The most challenging task for the RFID community is to get good publicity, because people's heads seem to be full of crazy ideas such as being tracked by satellite when carrying an RFID tag [10] (chapter 2). The public needs to be informed about the real possibilities of attackers, which are much less frightening then the horror scenarios which are brought to attention by RFID opponents (cp [20]).

After that, a new, secure protocol has to be designed or an existing protocol has to be assured to be secure and then it has to be made a standard for the tag/reader communication. When a secure, non-traceable technique is implemented, the public will accept RFID labels as they have accepted bar codes back in the 60s.

It is always good for the trust in a new technology, if one can 'see' that something is happening. Such an approach is realized with the privacy protection tag, which is described in Section 4.5 and [15]. The customer's trust gains a physical basis by crippling the tag by himself, also it would be very inconvenient to detach the antenna on every piece of grocery you buy. The killing, which we described in Section 4.1 is also a very confidence-building process but then the customer loses all the advantages of tagged items.

A solution could be to have a tag with two antennas, one for short range (a few centimeters) and one for long range (some meters). This tag could also have two completely independent memory systems, then the long range tagpart could be killed at the supermarket checkout and the hardly traceable short range tagpart could be used by the consumer for his own applications. It is questionable if this approach is realizable with reasonable costs but it could be interesting to be further researched.

As we have shown, RFID technology is an interesting field of research with important privacy and security issues, which have to be solved in the future.

Appendix: Classes of Tags as Defined by EPC

References

1. *http://www.engadget.com/entry/1234000257034127/.*
2. Cryptology ePrint Archive, Report 2005/052. *http://eprint.iacr.org/2005/052.*
3. Electronic Frontier Foundation. *http://www.eff.org/Privacy/Surveillance/RFID/.*
4. RSA Security. *http://www.rsasecurity.com/rsalabs/node.asp?id=2120#18.*
5. RFID Journal, Nokia unveils RFID phone reader. March 2004.
6. G. Avoine. Adversarial Model for Radio Frequency Identification. Cryptology ePrint Archive, Report 2005/049, Feb 2005.

EPC Device Class	**Definition**	**Programming**
Class 0	'Read only' passive tags	Programmed by the manufacturer
Class 1	'Write-once, read-many' passive tags	Programmed by the customer; cannot be reprogrammed
Class 2	Rewritable passive tags	Reprogrammable
Class 3	Semipassive tags	Reprogrammable
Class 4	Active tags	Reprogrammable
Class 5	Readers	Reprogrammable

Table 1. EPC RFID Classes

Band	**Unlicensed Frequency**	**Wavelength**	**Classical Use**
LF	125-134.2KHz	2400 meters	Animal tagging and keyless entry
HF	13.56MHz	22 meters	Animal tagging and keyless entry
UHF	865.5-867.6MHz (Europe) 915MHz(U.S.) 950-956MHz(Japan)	32.8 centimeters	Smart cards, logistics and item management
ISM	2.4GHz	12.5 centimeters	Item management

Table 2. Band Frequency, Wavelength and Classical Usage

7. G. Avoine and P. Oechslin. RFID Traceability: A Multilayer Problem. In *Procs. of Financial Cryptography and Data Security FC'05*, Roseau, The Commonwealth of Dominica, Feb 2005.
8. C. Castelluccia and G. Avoine. Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags. In *Procs. of International Conference on SmartCard Research and Advanced Applications CARDIS'06*, Tarragona, Spain, Apr 2006.
9. Kirk Dustin. How To Make A RFID Blocking Wallet. Cryptology ePrint Archive, Report 2005/049, Jan 2006.
10. S. Garfinkel and B. Rosenberg. *RFID: Applications, Security and Privacy.* Addison-Wesley Professional, 2005.
11. Simson Garfinkel. An RFID Bill of Rights. Technology Review. June 2002.
12. G. Hancke and M. Kuhn. An RFID Distance Bounding Protocol. In *Procs. of First IEEE/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm)*, Athens, Greece, Sep 2005.
13. Arik Hesseldahl. A Hacker's Guide to RFID. *http://www.forbes.com/home/commerce/2004/07/29/cx_ah_0729rfid.html*, July 2004.
14. F. Kahn. Can Zero-Knowledge Tags Protect Privacy? Cryptology ePrint Archive, Report 2005/049, Nov 2005.
15. G. Karoth and P. Moskowitz. Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced. *ACM Workshop on Privacy in Electronic Society (WPES)*, Nov 2005.
16. Ziv Kfir and Avishai Wool. Picking Virtual Pockets Using Relay Attacks on Contactless Smartcard Systems. 2005.
17. D. Molnar, A. Soppera, and D. Wagner. A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags. In *Procs. of Workshop on RFID and Lightweight Crypto*, Graz, Austria, Jul 2005.
18. D. Molnar, A. Soppera, and D. Wagner. Privacy For RFID Through Trusted Computing. In *Procs. of Workshop on Privacy in the Electronic Society WPES'05*, Alexandria, VA, USA, Nov 2005.
19. D. Ranasinghe, D. Engels, and P. Cole. Security and Privacy: Modest Proposals for Low-Cost RFID Systems. In *Procs. of Auto-ID Labs Research Workshop*, Zürich, Switzerland, Sep 2004.
20. Mark Roberti. RFID Opponent to Publish Book. Cryptology ePrint Archive, Report 2005/049, Jan 2006.
21. R.Stapleton-Gray. Would Macy's Scan Gimbels? Competitive Intelligence and RFID. *Stapleton-Gray & Associates, Inc.*, 2003.
22. R. Rivest S. A. Weis, S. Sarma and D. Engels. Security and privacy aspects of low-cost radio frequency identification systems. *In First International Conference on Security in Pervasive Computing*, 2003.
23. S.A. Weis. Radio-frequency identification security and privacy. Master's thesis, M.I.T. June 2003.

RFID Privacy and Security for ID cards and E-Passports

Hamid Reza Soleymani and Siamak Dehghani Zahedani

Databases and Distributed Systems Group
Dept. of Computer Science, TU Darmstadt, Germany

Abstract. RFID (Radio Frequency IDentification) tags are small, wireless devices that help to identify objects and people. The technology enables physical environments to become more interactive and supportive by tagging each item with a chip that wirelessly communicates with a service-enriched backend infrastructure. Due to low cost, they are likely to proliferate into a lot of number in the next several years. RFID systems are increasingly being deployed in industry and commerce. These contactless devices have raised public concern regarding violation of privacy and information security. There is a growing need in the RFID community to discover and develop techniques and methods to overcome several problems posed by the above-mentioned concerns. This paper surveys general problems of privacy and security for RFID.

1 Introduction

RFID, a chance or rather a time bomb? "Pervasive Computing" and "Ubiquitous Computing" respectively mark a new development in information and communication technology. "Pervasive" stands for "(everything) penetrating", "ubiquitous" for omnipresent. In future more and more things of the daily use will be equipped with microelectronic. The new emerging so called "Smart Objects" will nearly influence all area of every day life. Computers will complete their services increasingly invisibly and hidden in the background. Radio Frequency Identification (RFID) is one of those emerging technologies. In the next few years this technology will be deployed in the mighty industrial sector. Many big and small firms intend in early future to provide their goods, if yet not done, with this technology, hoping to organize their business process more efficiently. While on the one hand these positive commercial capability exist, there is an intense social debate on the implication of this technology. When RFID tags are attached to the products in retail and from there arrive homes, then it could result in a ubiquitous surveillance of people on the basis of their owned objects. Companies may be enthusiastic about this new possibility but the idea of integrated chips in objects surrounding us as well as the opportunity of quiet communication among each other calls a discomfort to many citizens.

2 Our goals in this paper:

In addition to other wireless technologies like sensor networks, wireless LAN, GSM and GPS, RFID technology is one of the important applications in information exchange today. In this paper we are dealing with security and privacy (S&P) of RFID based systems and we will present two applications where S&P must be assured prior to the use of RFID technology and we try to figure out whether S&P of RFID systems are different at all to traditional systems and if so, in which way. Exploring this, we will also show in which way these systems are threatened and therefore exposed to attacks. This paper will not discuss detailed cryptographic protocols but we will name some of them and give references for further reading.

3 What is RFID ?

The basic functionality of RFID systems is to provide identification of individual objects by the replies of the RFID tags. An RFID tag is a small microchip, with an antenna, holding a unique ID and other information which can be sent over radio frequency. The main idea behind it, is to attach an RFID tag to every object in a particular environment and give a digital identity to all these objects. The information can be automatically read and registered by RFID readers. The data received by the RFID reader can be subsequently processed for this specific object.

4 Definition of security and privacy:

Security is the protection of information systems and data from unauthorized (accidental or intentional) modification, destruction or disclosure. This protection also includes the confidentiality, integrity and availability of these systems and data.
Privacy is the ability of an individual or group to stop information about themselves from becoming known to people other than those whom they choose to give the information.

5 Security Services

A security service is a collection of mechanisms, procedures and other controls that are implemented to help to reduce the risk associated with a specific threat to a system. The most important security services are:

1. *Authentication*, which ensures that a system can only be accessed by individuals that are authorized.
2. *Confidentiality*, which ensures that information are not disclosed to unauthorized parties.

3. *Integrity*, which ensures that unauthorized parties do not modify data.
4. *Non repudiation*, which ensures that entities involved in a communication cannot deny having participated in it.
5. *Availability*, which ensures that a service is available at all times.
6. *Access Control*, which ensures that resources are being used in an authorized manner.

There are various mechanisms to ensure that the security services can be guaranteed.

5.1 Symmetric Cryptography

Symmetric cryptography, also known as secret key cryptography is based on encryption and decryption with the same key. The key and the plaintext are fed to an algorithm which generates the ciphertext. It is always assumed that the algorithm is known to the attacker but not the key.

Block Ciphers: Block ciphers break the plain text into blocks usually 8 or 16 byte long and operate on them independently. Usually the last block is padded with the number of pad bytes added so that the receiver knows which bytes to discard. Multiple appearances of similar text also results in similar patterns in the ciphertext. This can be avoided by using feedback modes. The most common feedback mode is the cipher block chaining (CBC) mode where the current block of plain text is XORed with the previous ciphertext.

Stream Ciphers: Stream ciphers generate a pseudo random key stream based on the key and XOR it with the plain text to generate the ciphertext. The key stream is independent from the input data. Decrypting is the same as encrypting because of the XOR function applied twice produces the original input. Stream ciphers are generally faster and use less code than block ciphers. The most common stream cipher RC4 is probably twice as fast as the fastest block cipher. Stream cipher keys should be used only once.

Symmetric Algorithms: Triple DES (Data Encryption Standard) is an adaption of the obsolete DES algorithm to meet modern security standards. It applies the DES algorithm 3 times and thus uses key lengths of 168 bits instead of 56 bits. Disadvantages of the 3DES algorithm are that encryption and decryption are very slow.

5.2 Asymmetric Cryptography

Asymmetric cryptography is also known as public key cryptography and applies two different keys. One key called the public key is used to encrypt data. The ciphertext can only decrypted by the second key: the private key.

Asymmetric Algorithms: The three most commonly used asymmetric algorithms are Rivest Shamir Diffie Hellmann (DH), and Elliptic Curve Diffie Hellmann (ECDH).

5.3 Digital Signatures

Digital signatures are used to authenticate the author of a message and to prevent people from going back on their electronic word (nonrepudiation).

Digital Signature Algorithms: The most commonly used digital signing algorithms are RSA (Rivest Shamir Adleman), DSA (Digital Signature Algorithm) and ECDSA (Elliptic Curve DSA), which is the same as DSA but based on elliptic curves. The following table summarizes "attacks and solutions" on security services.

Security Service	Attack	Solution
Authentication	Fake of identity	Passwords, tokens or a unique property
Confidentiality	Eavesdropping	Symmetric encryption, asymmetric encryption or both
Integrity	Modification of data	Checksums or Modification Detection Codes
Nonrepudiation	Fake of signatures	Public cryptographic techniques using digital signatures
Availability	Denial of Service attack	Redundancy, Quality of Service
Access Control	Unauthorized access	Hierarchical granular access and privilege architecture

Table: Summary of security services, attacks and solutions

6 Classification of Attacks

While there are many variations of specific attacks and attack techniques, their goals can be reduced to the following list:

1. *Spoofing* is the use of a false identity for example to get access to a system.
2. *Tampering* is the unauthorized modification of data.
3. *Information disclosure* is the unwanted exposure of private data.
4. *Denial of service* is the process of making a system or application unavailable.
5. *Elevation of privilege* occurs when a user with limited privileges assumes the identity of a privileged user to gain privileged access to an application.

The following table summarizes the security threats on RFID and Countermeasures.

Threat	Countermeasure
Spoofing	Strong authentication Store of secrets in encrypted or hashed form No passing of credentials in plain text
Tampering	Data hashing and signing Digital signatures Use of strong authorization Use of tamper-resistant protocols Secure communication links providing message integrity
Information Disclosure	Strong authorization Strong encryption Use of protocols that provide confidentiality
Denial of Service	Resource and bandwidth throttling Validation and filtering of input
Elevation of Privilege	Principle of least privilege

Table: Security Threats and Countermeasures

7 Fraud Scenarios in RFID Systems

For RFID systems the following general fraud scenarios can be identified:

7.1 Modification of Data

By unauthorized write access, the stored data on the tag can be modified. This attack is only effective if the identifier and security information such as keys remain unchanged. Otherwise this attack leads to denial of service. The attack is only possible if additional data next to the identifier are stored.

7.2 Tag Spoofing

In this attack an attacker gets access to a tags identifier and uses it to feign the original tag. This can be achieved either by emulating or by cloning. The requirement of uniqueness of tags is no longer fulfilled.

7.3 Deactivation of Tags

The tag is made inoperative by executing a dedicated command or by physical intervention. Depending on the degree of deactivation the identity or the presence of the tag can no longer be determined.

7.4 Removal of Tags

Under physical influence a tag is removed from the object, which is identified and maybe brought in association with another object. This is analogous to the exchange of price labels and violates the rule that a tag identifies its object.

7.5 Eavesdropping

The communication between tag and reader over the air interface is intercepted, decoded and interpreted.

7.6 Blocking

By the use of a blocker tag the presence of a arbitrary number of tags is simulated. A blocker tag has to be adapted to the specific collision protocol used.

7.7 Jamming

The data exchange over the air interface can be jammed either actively (jammer) or passively (shielding). Due to the susceptibility of the air interface even cheap passive methods can have an effect.

7.8 Reader Spoofing

In a secure RFID system readers have to prove their authority to read out tags. When an attacker wants to get access to the data on the tag, he has to feign an authorized reader. The following table shows that there are various intentions that attacks an RFID system might have.

	Protection of Privacy	Access to Data	Denial of Service	Spoofing
Modification of Data		X		
Tag Spoofing		X		
Deactivation of Tags		X	X	X
Removal of Tags		X		X
Eavesdropping	X			
Blocking		X	X	X
Jamming		X	X	X
Reader Spoofing	X			

Table: Intentions behind Attacks on RFID Systems

8 Security Threats Evaluated

When evaluating the security risks to RFID systems in the medium and long term, it is important to consider the costs an attacker has to spend as well the costs and efficiency of countermeasures. Rising fixed and variable costs with additional security mechanisms can be justified when a great number of pieces are produced.

8.1 Eavesdropping on the Air Interface

Without further security measures it is possible to eavesdrop on the air interface. The risk increases with the maximum reading range. For tags with a very short range the risk is relatively low. The costs for an attacker are high because he needs professional equipment and knowhow in the decoding of the data. Even though most communication over the air interface is standardized building a device for eavesdropping requires expert skills. Countermeasures include:

1. Shifting data into the back-end and storing only an identifier. This approach also facilitates data management.
2. Shielding zones where readers are used.
3. Encryption of communication over the air interface.

8.2 Unauthorized Access

To gain unauthorized access to a transponder, an attacker needs a stealth reader. This is not hard to accomplish, since most RFID systems comply to one of the currently existing standards. Moreover, RFID reading devices are easy to build, and will be easier to build as RFID technology spreads. Nokia unveiled (2004) a cell phone that can read RFID tags[5]. There already exist SD (Secure Digital) cards for Palm-compatible handhelds that can convert popular PDAs like the Treo into RFID readers[1]. German hacker Lukas Grunwald used his RFDump software on a PDA equipped with an RFID reader to read and write to RFID tags in a German grocery store[13]. In monitored areas attacks of this kind can be effectively prevented because range is limited. The construction of readers with longer ranges than the standardized one, requires expert knowledge. Countermeasures include:

1. Shifting data into the backend and storing only an identifier.
2. Detectors that can recognize readers.
3. Authentication.

8.3 Cloning and Emulation

Cloning is the creation of a new tag with data, that was previously obtained from a valid tag. This tag can then be used to spoof the identity of the original tag. Apart from that a device can be used to emulate any arbitrary tag (emulation). This way a smart shelf system can be fooled by replacing an items tag with a clone or an emulator. Countermeasures include:

1. All countermeasures against unauthorized reading.
2. Authentication.

8.4 Removal of Tags

Removal of tags is a trivial attack that can be easily carried out without equipment. Attacks of this kind target the relation between the tags and the item they identify. Intentions behind the removal of tags can be fraud or tampering. The risk of tampering is particularly high when it can be carried out easily and without detection. Possible countermeasures are:

1. Close mechanical link between tag and item.
2. Hiding tags in item.
3. Active tags with alarm function.
4. Additional identifiers (barcodes, watermarks)

8.5 Destruction of Tags

A destruction of tags can be accomplished mechanically or with an electromagnetic field. If tags are equipped with a kill command, an abuse of this command can also lead to an unwanted destruction of a tag. Therefore kill commands should be secured by authentication mechanisms to prevent unauthorized execution.

8.6 Blocking

In contrast to jamming the use of passive blocker tags is not prohibited by law. The available blocker tag from RSA is only applicable for RFID systems that use the tree-walking algorithm for anti-collision. For different protocols new blocker tags have to be designed and created, which is technically possible. So far there exist no technical countermeasures against blocker tags. The only way to prevent (legal) blocking is a prohibition in the terms and conditions of the system operator.

8.7 Jamming

Effective jamming from greater distances requires strong transmitters, whose unlicensed operation is illegal. For the general public it is hard to get access to the necessary equipment. Available countermeasures include:

1. Scanning for jammers.
2. Frequency hopping.

8.8 Shielding

Shielding can be carried out by wrapping the tag in a metallic foil. The problem with shielding is that it is relatively easy to do but impossible to rule out completely. Still, antennas from different directions and better readers may solve the problem partially. The following table lists attacks and possible countermeasures.

Attack	Costs	Countermeasures	Costs
Eavesdropping on the Air Interface	high	Data in Backend Shielding Encryption	medium
Unauthorized Reading	medium-high	Detectors Authentication	medium
Data Tampering	medium-high	Read-Only Tags Detectors Authentication	low-medium
Cloning and Emulation	medium	Duplicate detection Authentication	medium
Removal of Tags	low	Secure attaching Active tags with alarm Additional identifiers	low-medium
Mechanical or chemical destruction	low	Secure attaching	low-medium
Destruction with electromagnetic fields	medium	none	
Destruction with kill command	medium	Authentication	medium
Blocker Tag	low	none	
Jamming	medium-high	Detectors Frequency Hopping	medium-high
Shielding	low	Better readers	medium

Table: Security Threats and Countermeasures

9 Threats to RFID Privacy

An RFID system involves two parties with different interests. On one side, there is the system operator called the active party. The active party is in full control of the data and their use. It also issues tags and manages the data associated. On the other side, there are the employees and customers, referred to as the passive party. Usually the passive party has no influence on how the data on the tag is used. For the active party the correct function of the RFID system is vital, whereas for the passive party it is important that the advantages of the new technology outweigh its disadvantages. The rights on privacy are:[11]

1. The right to know whether products contain RFID tags.
2. The right to have RFID tags removed or deactivated when they purchase products.
3. The right to use RFID-enabled services without RFID tags.
4. The right to access an RFID tags stored data.
5. The right to know when, where and why the tags are being read.

9.1 Privacy Scenarios

Depending on the privacy right concerned it can be distinguished between data privacy and location privacy. Both are equally important to consider.

Data Privacy If an RFID system stores personal data the privacy of the passive party is threatened in the following ways:

1. By eavesdropping on the air interface or unauthorized reading of tags an attacker can gain access to personal data.
2. Next to personal data also potentially personal data can be the target of an attack on privacy. This includes data that are anonymized but can with high probability be dereferenced.
3. The high congruency between the real and the virtual world can awaken the interest of other parties in the data. It might for example be possible that the police legally enforces access to the collected data, which might not be wanted by the users.

Location Privacy Usually the passive party is in possession of RFID tags for a longer period of time. As a consequence an attacker is able to create a movement profile of the victim by reading out the static identifier on a regular basis. This is referred to as tracking. The danger of tracking rises when RFID is employed on a ubiquitous scale. In contrast to data privacy threats, no personal data is obtained except for the location. Tracking based on RFID tags provides no continuous data but is much more precise than the tracking of other radio based devices because reader ranges are small compared to for example base stations of cellular radio networks. Furthermore RFID tracking provides additional data such as the concrete type of interaction with an RFID infrastructure.

10 Evaluation

Many cryptographic models of security fail to express important features of RFID systems. For example, due to manufacturing variations, it is conceivable that an adversary could identify tags based on physical quirks in the signals they emit. Even the best cryptographic privacy-preserving protocol may be of little avail if an RFID tag has a distinct "radio fingerprint".

Most RFID tags emit unique identifiers, even tags that protect data with cryptographic algorithms. In consequence, a person carrying an RFID tag effectively broadcasts a fixed serial number to nearby readers, providing a ready vehicle for clandestine physical tracking. Such tracking is possible even if a fixed tag serial number is random and carries no intrinsic data. The threat to privacy grows when a tag serial number is combined with personal information. For example, when a consumer makes a purchase with a credit card, a shop can establish a link between her identity and the serial numbers of the tags on her person. It can be pointed out that mobile phones already permit wireless physical tracking, and are practically ubiquitous. But it must be considered that mobile phones, however, have on/off switches. More importantly, mobile phones transmit signals receivable only by specialized telecommunication equipment.

The owner of a mobile phone mainly reposes trust in his service provider and information about whereabouts (and calling patterns) is regularly available

only to service provider, a centralized and highly regulated source of information gathering. What makes RFID a more significant privacy threat in many ways than mobile phones is the fact that readers will be readily available and ubiquitously deployed. In other words, RFID readers will soon be an accepted element of everyday life (while eavesdropping equipment for mobile phones is unlikely to be)[4].

11 ID cards

An identity document is a piece of documentation designed to prove the identity of the person carrying it. If an identity document is in the form of a small standard-sized card, it is called an identity card. RFID tags are designed for convenience of reading but that convenience comes with a high cost to privacy and a high risk of identity theft[3]. It believes that in the vast majority of applications, ID cards that require physical contact with a reader will meet organizational goals with far less harm to privacy.

11.1 Privacy threats

1. *Unintended or unauthorized disclosure of personal or sensitive information:* The most obvious threat is that information might be read from a card for inappropriate use without the holder's knowledge or consent. Any compatible reader within range of the RFID tag could read the stored data. Read range varies depending on the radio frequency being used, the power of the reading device and many environmental factors. Eavesdropping is a second type of information disclosure threat. In eavesdropping, the attacker does not read the information directly from the RFID tag or card; instead, the attacker listens to the transmission between the RFID tag and an authorized RFID reader. Researchers have described an eavesdropping "relay attack" using two devices: a "leech" that can be as far as 50 centimeters from the RFID device, and a "ghost" that can be up to 50 meters away from the authorized reader[16], [2]. The eavesdropping threat is the main reason why merely shielding RFID devices is inadequate to protect privacy, because the RFID card must be exposed in all legitimate transactions.
2. *Clandestine tracking:* An RFID card also enables others to secretly monitor its holder's whereabouts and possibly his or her actions. As the number of RFID readers in the social environment increases, the easier it will be to track RFID tags. Importantly, the tracking threat exists even if the RFID tag contains no name or other personal information. What matters is that the RFID tag contains a static unique number or pattern that is or can be persistently associated with a person's identity. So long as the RFID tag or chip broadcasts this information, the person carrying that tag can be distinguished from any other person carrying a different RFID tag. For example, suppose the RFID tag in your ID card always transmits the number 0001. Anyone with a reader within range can read 0001 from your card, and

can distinguish you from someone carrying a card that transmits 0002. The reader owners need only know that you carry the card that transmits 0001 in order to track you. Note also that the tracking threat is not merely a real-time threat. Someone may record 0001 in multiple locations without knowing that you are 0001. But once they associate 0001 with you, then they know where you have been. And there are many ways to associate you with 0001.

3. *The "key" problem:* Any unique ID number on the card may be a "key" to personal information stored in a database somewhere. Our society often uses unique ID numbers to index or organize personal information in databases or as a linking or matching identifier across multiple databases. The worst-case scenario would be a commonly used unique number like a Social Security number, phone number, or a driver's license number, which is already used to index and link personal data. But even if a new unique ID number was generated for RFID cards that number would presumably act as a "key" to the individual cardholder's information in the database. Unless strict precautions against "function creep" were taken, any new unique ID number could very well become widely used as a "key" to data about card's holder.

11.2 Security threats

RFID tags also present security issues, such as "cloning" or duplication and card forgery. If the RFID tag is read but the card itself is not examined, cloning the RFID tag alone might suffice for an illegitimate purpose. This could easily occur in "walk-through" application when the card is read from one's wallet, pocket or purse, or in "self-service", automated contexts when no person actually looks at the card. If the RFID tag is read while the card is presented but not examined closely, cloning the tag or even forging the tag combined with a stolen blank card or a forgery of the actual card might be enough. Encryption, access control, and other techniques can be very difficult to implement properly and are especially unlikely to succeed in the real world of mass applications(applications with large numbers of devices and users, large number of authorized readers, and large numbers of authorized uses). The general problem of security for mass applications is relatively simple: when many entities are entitled to decrypt or otherwise access the protected information, it is very hard to keep that information protected.

Problems with encryption

1. Even if the data stored on the RFID card is encrypted, an enormous number of authorized users (whether state or local officials or commercial users) would be in a position to abuse their authorized access to the data. If the data were read directly from the cards themselves, rather than from a central database, it would be difficult to maintain an audit trail of access to the data, and therefore very difficult to detect abuse.
2. Even if the data stored on the RFID card is encrypted, an attacker could eavesdrop on a legitimate data transmission between the RFID card and the

RFID reader. For instance, if the system was designed so that RFID card only transmits after it receives a secret code or PIN from a legitimate RFID reader, an attacker could capture the PIN while it is being sent. Alternatively, if the data on the RFID card is encrypted while stored, but is transmitted in decrypted form, an attacker could capture the decrypted data when it is being sent to the RFID reader.

3. By definition, every authorized RFID reader can decrypt the data stored on RFID card. Thus, many thousands of readers would have access to the keys needed to read the RFID cards. There are two main scenarios here. a) If every card is protected by the same encryption key or PIN , then each reader would need to have that PIN or key. It is essentially impossible to maintain the confidentiality of such widely distributed information. One might also steal the PIN or key from inside the system. Storing the key in an attached computer system, rather than in the reader hardware itself, makes this attack easier, not harder. The computer is just as easy as the reader to steal, and generally easier to extract the key from. b) If a different PIN or key was used for each card, then readers would need access to the PIN or key for each card read. This creates enormous complexity and logistical problems, as well as a large set of difficult security concerns. For instance, suppose that each RFID card's PIN or encryption key is kept in a central database that authorized RFID readers could access. The implications include:

   - It would be impossible to use RFID readers without some communication channels to the central database, possibly making the readers unusable in many field applications.
   - Any such communications channels would need to be protected against eavesdropping.
   - Complicated access control and authentication mechanisms would be needed to ensure that queries to the database truly came from legitimate readers.
   - It would still be possible to steal or "borrow" and abuse a legitimate reader.

4. Encryption transforms the original information into different information but the result will still be unique. Accordingly, encryption cannot solve the tracking problem because encrypting unique information will result in different but still unique, information.
5. Encryption does not protect against cloning. To clone the data stored in an RFID tag, it is only necessary to copy the encrypted data verbatim from one chip to another. One need not be able to understand the data. Furthermore, static digital signatures or certificates do not prevent cloning. A digital signature proves only that the data is the same as the data signed by the signing authority. Copying the entire contents of the chip, including the digital signature, will create a card that appears as valid to verifying software as the original, unless additional precautions are taken.

12 e-Passport

Under the pressure of american administration, the next generation of passports are supposed to contain personal information and some biometric criteria in digital form. This information ranges from names over passport photograph to iris attributes and fingerprints. All these information is to be accommodated in a chip, which is then embedded in a RFID tag into the passport.This information stored on the RFID tag can be later read out by an interrogator.For example in airports to gain access control for security relevant areas.

12.1 The goals of e-Passport

The goal is to provide strong authentication through documents that unequivocally identify their bearers. Data integrity and physical integrity are vital to the security of passports as authenticators and strong authentication requires more than resistance to tampering. Data confidentiality, i.e. secrecy of data stored on e-Passports, is also critical. Protecting biometric and biographical data is essential to the value and integrity of an authentication system. In particular, data secrecy needs an important form of protection against forgery and spoofing attacks. Therefore protecting e-Passport data against unauthorized access is a crucial part of the security of the entire system. Together, RFID and biometric technologies promise to reduce fraud, ease identity checks and enhance security. How can we permanently protect these highly privacy-sensitive data against unauthorized access and data tampering, then missing to protect this personal information, it will be very easy to scan those sensitive data with a (portable) Reader.
Any kind of data, which is stored on a RFID tag is to be considered either as public accessible or must be provided with access control no matter in which concrete form. As mentioned above RFID tags have to be protected in e-Passports against physical attacks and most notably nobody should be able to track the bearer of the e-Passport.

12.2 Threat to location privacy

Assuming that tags will remain in the possession of the same person over long periods of time, (as given here by e-Passport) repeated reading of IDs allows movement profiles (tracking) to be generated. This possibility becomes a threat to privacy if and when RFID systems become a ubiquitous part of everyday life. Even if nothing but IDs are transmitted during the readout of RFID tags, while all other data are shifted to the backend, a threat to privacy can result. The more tags there are in circulation, the better chances that tracking can be carried out. Tracking more than one person also allows contact profiles to be established. A specific characteristic of RFID is the possibility of eavesdropping on the air interface. On the other hand, the possibility cannot be excluded that attacks in the backend area pose a bigger threat to privacy than attacks at the air interface. Compared to the use of mobile telephones, the use of RFID tags

generates more precise data traces, because not only the geographical location but also the concrete interaction with existing firms and infrastructures can be determined.

12.3 The Encryption approach

For applications where relevant contents have to be stored on the tags themselves, only strong encryption procedures can provide reliable protection against eavesdropping. The effectiveness of cryptography is based upon its key bits length. However, Steve Bono and Matthew Green demonstrate in how they succeeded in defeating the security of an RFID device using inexpensive off-the-shelf equipment, and with minimal RF expertise. This suggests that an attacker with modest resources can emulate a target RFID after brief short-range scanning or long-range eavesdropping across several authentication sessions. They concluded that the cryptographic protection afforded by a RFID device is relatively weak. Three instances of the Encryption approach that have been proposed are the hash-lock method, the re-encryption method (in several forms) and silent tree-walking. These approaches are exceptionally challenging to design, due to severe cost constraints. As example we explain only the Hash-Lock.

Hash-Lock In this approach, according to Weis et al. [22] [23], a tag may be "locked" so that it refuses to reveal its ID until it is "unlocked". In the simplest scenario, when the tag is locked it is given a value (or meta-ID) y and it is only unlocked by presentation of a key or PIN value x such that $y = h(x)$ for a standard one-way hash function h. To make this approach workable, it may be necessary for a reader to query a tag to find its meta-ID, so that the reader knows which PIN to use to unlock it. But this may allow tracking of tags via their meta-IDs, defeating their whole purpose. Weis et al. show how to use randomization in the hash function computation to solve this problem. While this is an effective approach, it seems likely that consumers will find it inconvenient to manage the lock/unlock patterns and associated PINs of more than a small collection of tags.

The Faraday Cage approach To prevent skimming, the new e-Passport will have shielding material on the passports front cover. So the passports front covers an anti-skimming material that blocks the radio waves that could pick up the data. This shielding material is based on Faraday cage and makes the e-Passports RFID tag unreadable as long as its cover is closed or nearly closed. Combined with access control lists, this approach could be a good solution for preventing tracking of a person and eavesdropping of the communication between reader and the e-Passport's tag. As always, its not a 100 % protection of the sensitive personal data. An attacker could hijack the communication between reader and the tag even in a short time. There is no protection of the RFID tag directly. The protection is given through protection of the product, in which the RFID tag is embedded to protect the RFID tag. The implementation of access control lists for protecting personal information is in fact needed but also complex and expensive.

The "Shift the data to the backend" approach The most effective protective measure against an attack involving eavesdropping at the air interface is, however, not to store any contents on the tag itself and instead to read only the ID of the tag. The data associated with the tag are retrieved from a backend database. This approach, which is most often recommended in the technical literature and which is proposed by EPCglobal, offers the additional advantages that less expensive tags can be used and memory for the associated data in the backend is practically unlimited and the usual procedures for data management and IT security can be employed. For instance cryptographic methods with their strong keys and real public key infrastructure (PKI).
So far, we have seen a few approaches for S&P. Which of them is suitable depends on the concrete application.

13 Summary

In this paper we tried to explain the impact of RFID enabled systems on our daily life. We showed which risks and attacks are generally possible on this infrastructure and presented some countermeasures to protect this system. We pointed out the two kinds of protection namely protection of the RFID tag as carrier of whole data using encryption and protecting it through shielding or backend systems. Both approaches have its assets and drawbacks. The best approach would be a combination of both for instance shielding and encryption. We come to the conclusion, that cryptography does not yield the kind of protection like in other applications, due to capacity of RFID chips.

References

1. *http://www.engadget.com/entry/1234000257034127/.*
2. Cryptology ePrint Archive, Report 2005/052. *http://eprint.iacr.org/2005/052.*
3. Electronic Frontier Foundation. *http://www.eff.org/Privacy/Surveillance/RFID/.*
4. RSA Security. *http://www.rsasecurity.com/rsalabs/node.asp?id=2120#18.*
5. RFID Journal, Nokia unveils RFID phone reader. March 2004.
6. G. Avoine. Adversarial Model for Radio Frequency Identification. Cryptology ePrint Archive, Report 2005/049, Feb 2005.
7. G. Avoine and P. Oechslin. RFID Traceability: A Multilayer Problem. In *Procs. of Financial Cryptography and Data Security FC'05*, Roseau, The Commonwealth of Dominica, Feb 2005.
8. C. Castelluccia and G. Avoine. Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags. In *Procs. of International Conference on SmartCard Research and Advanced Applications CARDIS'06*, Tarragona, Spain, Apr 2006.
9. Kirk Dustin. How To Make A RFID Blocking Wallet. Cryptology ePrint Archive, Report 2005/049, Jan 2006.
10. S. Garfinkel and B. Rosenberg. *RFID: Applications, Security and Privacy.* Addison-Wesley Professional, 2005.
11. Simson Garfinkel. An RFID Bill of Rights. Technology Review. June 2002.

12. G. Hancke and M. Kuhn. An RFID Distance Bounding Protocol. In *Procs. of First IEEE/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm)*, Athens, Greece, Sep 2005.
13. Arik Hesseldahl. A Hacker's Guide to RFID. *http://www.forbes.com/home/commerce/2004/07/29/cx_ah_0729rfid.html*, July 2004.
14. F. Kahn. Can Zero-Knowledge Tags Protect Privacy? Cryptology ePrint Archive, Report 2005/049, Nov 2005.
15. G. Karoth and P. Moskowitz. Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced. *ACM Workshop on Privacy in Electronic Society (WPES)*, Nov 2005.
16. Ziv Kfir and Avishai Wool. Picking Virtual Pockets Using Relay Attacks on Contactless Smartcard Systems. 2005.
17. D. Molnar, A. Soppera, and D. Wagner. A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags. In *Procs. of Workshop on RFID and Lightweight Crypto*, Graz, Austria, Jul 2005.
18. D. Molnar, A. Soppera, and D. Wagner. Privacy For RFID Through Trusted Computing. In *Procs. of Workshop on Privacy in the Electronic Society WPES'05*, Alexandria, VA, USA, Nov 2005.
19. D. Ranasinghe, D. Engels, and P. Cole. Security and Privacy: Modest Proposals for Low-Cost RFID Systems. In *Procs. of Auto-ID Labs Research Workshop*, Zürich, Switzerland, Sep 2004.
20. Mark Roberti. RFID Opponent to Publish Book. Cryptology ePrint Archive, Report 2005/049, Jan 2006.
21. R.Stapleton-Gray. Would Macy's Scan Gimbels? Competitive Intelligence and RFID. *Stapleton-Gray & Associates, Inc.*, 2003.
22. R. Rivest S. A. Weis, S. Sarma and D. Engels. Security and privacy aspects of low-cost radio frequency identification systems. *In First International Conference on Security in Pervasive Computing*, 2003.
23. S.A. Weis. Radio-frequency identification security and privacy. Master's thesis, M.I.T. June 2003.

Smart Objects

Hauke-H. Vagts and Barbara Wasilewski

Databases and Distributed Systems Group
Dept. of Computer Science, TU Darmstadt, Germany

Abstract. The technological development of embedded processors, memory, sensors and networking made the development of the RFID technology possible. Small and cheap tags can be attached to real objects, which can then be detected by tag readers. Computers process the information transmitted by these tag readers. By having a tag attached, real world objects are introduced into the IT world. On the other side further trends will enable inserting IT into real world objects, which will make them smart. In this paper we will present some applications of smart objects. Our focus is on describing their infrastructures and how they handle the challenges arising from smart objects.

1 Introduction

Smart objects are real world objects, which are equipped with a tag and maybe with a processing unit. They can communicate among each other and with connected IT systems, whereas the actual technical state of affairs allows the detection of tagged objects, but not so much the communication among them. Today's processing units for smart objects are too expensive and too obtrusive to be implemented in everyday's objects. Therefore today's smart objects are passive objects, which can be detected but they do not act themselves. The "smartness" is implemented in the software infrastructure or by adding it to components in the objects' environment. Roughly speaking, today the applications are smart, the objects themselves less so. But in future the technological developments will certainly make the objects themselves smart.

This trend will be picked up in our following description of applications with smart objects. At first we will present a list of properties, which are common for application with smart objects. Then we will describe a smart kitchen counter. The counter detects the tagged groceries, which are placed on it. Recipes which can be prepared with the tagged groceries are suggested by a monitor. In this application focus is on the software infrastructure since it implements the groceries' "smartness". An overview over a technical infrastructure is given with the second application, a smart kindergarten. The idea of the smart kindergarten is to provide an environment for children where they can learn by exploring and interacting with objects, mostly with toys. The smart kitchen counter and the smart kindergarten are designed for research purposes. An application in the area of economy is the baggage management at airports. This application shows the

cost effectiveness of smart applications by increasing the performance of baggage handling and decreasing the costs caused by wrongly delivered baggage. The last application describes the benefits of smart objects in the maintenance of airplanes. Smart objects can be used to automate the maintenance process and avoid human errors.

2 Properties of Applications with Smart Objects

The Distributed Systems Group of the ETH Zurich[1] implemented some simple smart applications for research interests. Their goal was to build a framework for applications that use the smart identification technology. For these purposes they analyzed common properties of smart applications. We will list the properties in this section and describe them shortly. The following applications will take up some of them.

- *Location and Location Management.* An important issue is the determination of an object's position. It can be specified as geographic coordinates or as a symbolic position like a room number. Symbolic positions can be organized hierarchically (for example a building number combined with a room number) and can change over time. Two rooms for example can be merged to one single room. While determining the position it must be considered, that some objects can contain other objects and that it can change dynamically.
- *Neighborhood.* This is a relation between objects, which are close to each other and which probably will deal with each other.
- *Composition.* In some applications it can be useful to compose an aggregation of several objects to one single object. For example to aggregate several bottles of water to one water box. The composition should be a static concept.
- *History.* The history of objects can be logged and queried. In case of the airplane maintenance for example the date of each maintenance can be logged for every tagged part of an airplane.
- *Context.* Not all detected objects are relevant for an application. Consider the smart kitchen and a cook, who prefers vegetarian food. In this case it won't be necessary to detect meat products.
- *Identification.* Every object will need an unique identification number.
- *Linking physical and virtual world.* Physical objects, which are by tag readers or other sensors has to be linked into the virtual world. The detection and linking is based on two events: entering and leaving of an object in the range of the reader or sensor. If an object is detected it can be linked by creating a virtual counterpart, which will represent the object in the virtual world.
- *Life cycle Management.* If a tagged object is destroyed, it's virtual representation can be destroyed too or can be saved.

[1] ETH Zrich, Department of computer Science, Distributed Systems Group: www.vs.inf.ethz.ch

3 Smart Kitchen

Motivation As mentioned in the last section the Distributed Systems Group of the ETH Zurich[1] implemented a smart kitchen counter for research interests. The kitchen counter can register tagged groceries placed on it and suggest recipes that can be prepared with them.

In this application the real world objects (the groceries) are not smart. Instead the object's smartness is put into the virtual world. Each tagged object has one virtual "proxy" object assigned to it. This way real objects have only to be tagged for identification purposes. Sensors don't have to be integrated into the objects themselves, but can be placed in the environment. There the sensors can detect the presence and status of objects and transfer this information to the proxy object. The proxy object can process the information and furthermore offer services, which make the application smart. Regarding the costs and todays technological possibilities of making real objects themselves smart, smart proxy objects are a cheap alternative.

Technical Infrastructure The focus of the kitchen counter application is on developing a software infrastructure. Therefore the technical components are not chosen under an unobtrusive and user-friendly aspect.

An illustration of the technical infrastructure is shown in Figure 1. The basis is Philip's I-Code tag system [2]. Each groceries item is tagged with a unique RFID label, which are placed over the barcode position. This simulates future packaging where barcode labels will be equipped with RFID tags. In this application each tag has 64 bits of read-only memory and 384 bits of read-write memory. The tags are detected by the RFID reader's antenna, which is mounted underneath the kitchen counter. The reader can read or write within a range of 1x1m up to 30 tags. The reader is connected to a standard PC via a serial cable. An LCD monitor displays the recipes.

Software Infrastructure The kitchen counter's software infrastructure is shown in Figure 2. It is based on events, which for example occur if a grocery item is placed on the kitchen counter. An event is a message created by an event source and send to an event consumer. As a response the event consumer executes an action or generates another event. In the example the RFID reader serves as the event source, which sends a message to the PC, the event consumer, when it detects a grocery item in its range. The PC responses by creating the proxy object. Events like detecting objects are called basic events. They can be directly or indirectly generated by the sensory hardware. More complex events, called context events, can be generated by the aggregation of one or more basic events (or the aggregation of other context events).

[1]

[2] Philip's I-Code Systemwww-us2.semiconductors.philips.com in Product Information/Identification/Icode

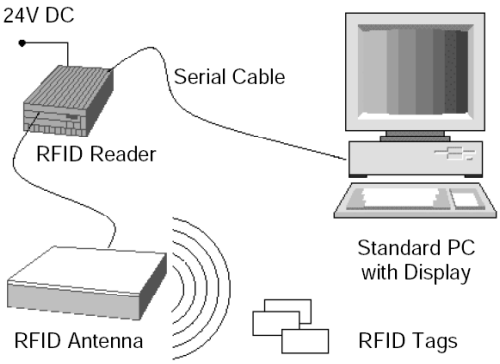

Fig. 1. Technical infrastructure of the kitchen counter application

As shown in Figure 2 events pass through different layers. The lowest layer is the *Sensory Control and Input Processing Module*. It scans the sensors (in this application the RFID reader) continuously for information regarding their status and detected objects in their vicinity. The information is forwarded at discrete time intervals to the Basic Event Modeling Module. Besides the Sensory Control and Input Processing Module configures and controls the sensory hardware. This can be affected by higher-level context events.

The *Basic Event Modeling Module* creates basic events, which can be directly generated by the sensory hardware. For creating appearing or disappearing events a list of lastly identified tags is stored. The list is then compared to a list of currently detected tags. If the lists differ, corresponding events are generated. The basic events are then passed to the next layer, the Context Event Modeling Module.

The *Context Event Modeling Module* is responsible for processing, filtering and combining basic events to context events. The context events then make the processing of events at a higher granularity possible. If for example new groceries are placed on the kitchen counter, several appearing basic events are generated. These basic events are then combined to one single context event, which causes the displayed recipe list to refresh only one time. Otherwise the recipe list would be reordered for every new grocery item, which could lead to a repeated flickering on the LCD monitor. Similarly basic disappearing events are not immediately processed by the module, but held back for sometime. In case the corresponding removed grocery item is only rearranged and therefore placed back on the kitchen counter after sometime, no unnecessary reordering of the recipe list has to be done.

Outlook The kitchen counter application was implemented for research interests. Therefore it is a simple application with a few tagged objects, which besides

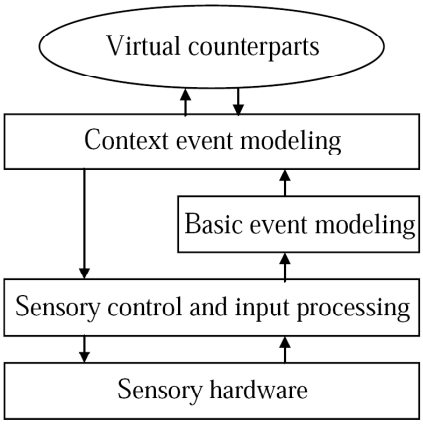

Fig. 2. Software infrastructure of the kitchen counter application

don't communicate with each other. It is a challenge to add a complex interaction model to the application, which allows communication between the objects themselves and more interaction possibilities for the users. The communication between objects can be realized by adding sensors and processing units to the objects. In this case the objects become expensive. Another possibility is to extend the existing application and to add the communication abilities to the proxy objects. The real objects will then react depending on their proxy object's communication. In this case the processing of the information, which is transfered between the real and proxy objects, must be nearly in real-time. A challenge will then arise, if we assume that the proxy and real objects are distributed locally.

In the next section an application is described, which has a more complex interaction model, which is realized by different sensors. There the focus will be on the technical infrastructure.

4 A Smart Kindergarten

Motivation The existing development of computer and networking technologies made a "person-to-computer" and a "person-to-person" communication possible. In future the decreasing sizes and costs of technical components will allow a "person-to-physical world" communication.

In this section we will describe a smart kindergarten. In this application children will communicate with toys and other objects and the objects will be able to react. The goal of a smart kindergarten is to offer an environment for children, in which they can learn by exploring and interacting with the included objects. The vision is to make a learning environment available, which is adapted to each child individually and can manage a group of many children. The progress of each child can be evaluated by the teacher. For this reason objects like toys

are equipped with sensors, which communicate with databases and middleware services using a wireless network. For example a toy may be able to sense speech or physical manipulation and to react visual or by a motion.

In this manner the smart kindergarten is not implemented. It is designed for research interests. The focus is on working out the challenges, which arise for the networking infrastructure, the middleware services and the database management regarding this application. Nevertheless a technical infrastructure is described, which can be used in applications with different smart objects.

System Architecture The smart kindergarten contains a lot of objects, which are equipped with sensors. Connecting them with a wired network would be inflexible and obtrusive. Therefore the objects communicate using a wireless network with an underlying infrastructure, that provides storage and processing units. Some sensors have only sensing capabilities and some are able to process their data. In this application with many different objects and sensors it is useful, that some processing is done locally, like filtering important information or converting information into another format. The architecture is restricted in the areas of power management, computation, storage and communication capabilities of the technical components. Figure 1 shows the technical infrastructure of this application.

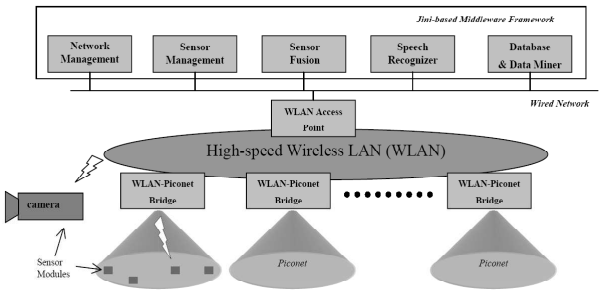

Fig. 3. Network and Service Infrastructure for the Smart Kindergarten

Sensing Infrastructure Sensing components in this application are controllable cameras, which are mounted on the walls, microphones and speakers, which are positioned at strategic places, and objects like toys, which are equipped with sensors for touch and pressure. Children may also have microphones for feedback and localization reasons. The localization has to determine the absolute position as well as the relative position, for example if a child is near a toy or another child. The cameras have to react on events. Based on sensor information like speech or motion they have to put their focus on events of interest. This means

that the sensor information has to be filtered such that interesting events can be detected. The microphones and speakers have several functions. They can be used as communication components, where the speakers can give instructions to control the children's actions and the microphones can receive feedback. The different signal strengths of the microphones can be used as an additional sensory mechanism for the localization of the speaker. If the signal strength is low, then the speaker is probably far away. The redundant information collected by several speakers can help the speech recognition process. By combining the redundant information interferences can be detected and filtered out.

Wireless Networking and Middleware Services The networking infrastructure contains wireless connected components. As shown in Figure 3 it is organized in two layers: the piconets and the high speed wireless LAN. Piconets are small overlapping units, which cover several sensored objects. (The name piconet is borrowed from Bluetooth's jargon.) The objects can communicate in a short range and their technical equipment is not expensive. The communication is realized by Bluetooth for example. The WLAN layer enables a fast communication and has a longer range. Piconets can communicate with the high speed WLAN via custom bridges. This means the objects within a piconet localize the nearest bridge and starts the communication. The high speed WLAN then transfers the information via an access point to the corresponding middleware services. Objects with a lot of sensor information, like cameras, are connected directly to the high speed WLAN.

Research challenges arise because present wireless access protocols has to be worked over to deal with a large number of networked devices and with the large diversity of rates. Besides some devices have streaming requirements, while others have low latency constraints. For all devices an energy efficient access has to be enabled.

The middleware services are organized in a wired network. The middleware provides services like allocating, access control and scheduling of the networking resources as well as media specific information processing like speech recognition and collection of context information.

Sensor Data Management Services The challenges, which arise for the data management, mainly result from the large amount of different sensor data. Services for the data management in the smart kindergarten application must be able to extract important information from the sensor data. But it is not known beforehand, which sensor data will be available and which not. Data structures have to be developed, which allow to query, mining and browsing a repository with video, audio and other sensor data. Also different timescales have to be taken into consideration. For example a toy has to react in real-time to a child's action. But the evaluation of a child's learning process is allowed to take a longer time. A suggested software infrastructure for the sensor data management is shown in Figure 4.

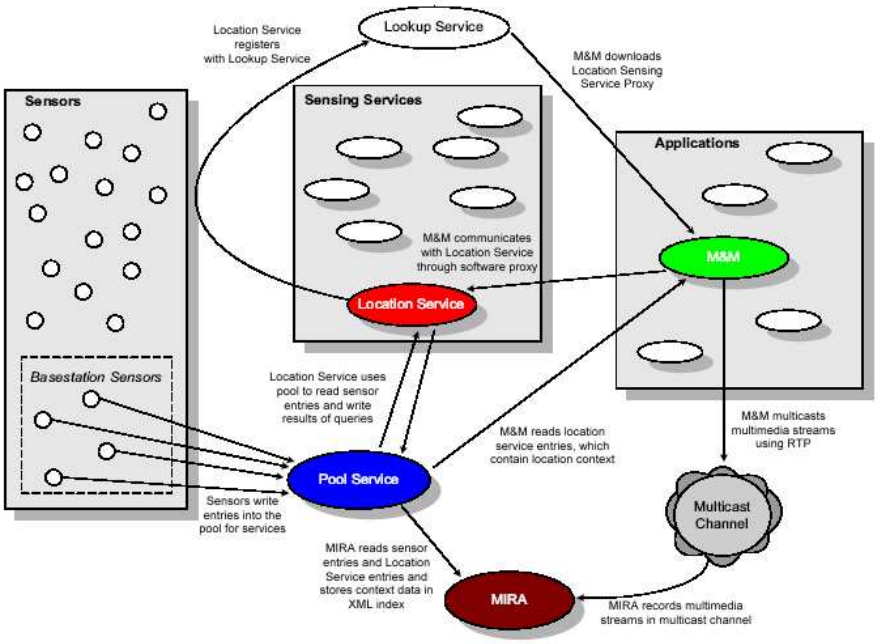

Fig. 4. Software Infrastructure for the Smart Kindergarten

Data, which is collected from the sensors is stored in a pool. Sensing services like location services for determining the position of objects or registration services for new available sensors can access the stored data. A module (called MIRA module) reads the data from the pool and stores it in an XML fomat. The advantage of using XML is, that the data can be flexibly indexed, queried and browsed. Data from audio or video devices is stored in separate objects to ensure a real-time delivery. It is transferred using RTP[3], which is a protocol for a continuous transmission of audio-visual data.

The mentioned sensing services are responsible for reading the sensor data from the pool and add additional information, which is then stored together with the raw sensor data. For example a location service reads the position of a child from the pool. It then compares the child's position to the positions of all registered toys in the same room and adds the position of the closest toy to the child's pool entry. All sensing services are registered in a lookup service. If an application requests a service, a service proxy is assigned to it, which manages the communication. Using software like JINI[4] it is possible to create sensing services dynamically, which makes the kindergarten application scalable to adding new sensor devices.

[3] Real-time transport protocol: http://www.ietf.org/rfc/rfc3550.txt
[4] JINI: http://www.sun.com/software/jini/ and http://www.jini.org

Outlook Unlike the smart kitchen counter application the smart kindergarten has more objects with different sensor data. Since the application was also designed for research interests many challenges are described without offering a solution yet, like algorithms and filter for handling the huge amount of sensor data, new networking protocols for many different devices and data models to support the variety of sensor data.

In the next section the applications are not developed for research but for economical usage. We will describe these applications and show their economic importance.

5 Baggage Management

Motivation The idea to use RFID for a better Baggage Tracking is not new, airlines have been thinking about it for about fifteen years, but the higher cost has prevented airlines and airports to move to RFID Systems. Nowadays the falling price of RFID tags, the requirement in the United States to screen all bags for explosives (after 11/09/2001) and the increasing quantity of baggage, have made RFID to an interesting technology for saving money. Therefore, it is no wonder, that "The international Air Transport Association" (IATA) [5] is driving force behind the efforts the use of RFID, as part of its 'Simplifying the Business program'.

McCarran International Airport McCarran International Airport (Las Vegas) was the first airport to announce the use of RFID-technology for an airport-wide routing and sorting system. After about 2 years (last November), they have finished the first deployment phase and are currently running the second one.

The personal at McCarran has to handle about 65,000 - 70,000 bags per day. With barcode-technology 15-30% were misscaned. If 15% (9750 bags) are deliverd incorrectly, all of them have to be rerouted manually at a high cost of manpower! With RFID-technology you can get read accuracy rates up to 99.5% (in William Gibbs [6] opinion), which save a lot of manpower. The main reason for the better scanning rate of RFID-tags is, that the orientation of the bag is not important, in fact it isn't necessary to see the tag or the item itself. Another advantage of RFID-readers is the price. Costing a "few" thousand dollars they are really cheap (compared to 360-degree barcode scanners), this allows a higher resolution in the monitoring process. With lower missrates and cheap readers, it is possible to build an infrastructure, that has a higher capacity and better performance. A positive side effect is, that fewer bags are missing. This leads to a better service for the passangers and savings for the airlines.

Only a RFID-tag does not make an item smart, you need a smart software, to controlls the environment. So you need smart software to help bags to get to

[5] The association brings together 265 airlines, including the world's largest. http://www.iata.org

[6] Swanson Rink's senior mechanical engineer and the controls engineer for the McCarran project. http://www.rink.com/

theirs flights. A reason for bags missing flights is that a bag that arrives too early, must be stored and is then forgotten. A smart System detects early baggage items and sends them to an Early Baggage Storage. The baggage remains here under the supervision of the monitoring system. When the right plane is accepting luggage, the bags get routed there. The monitoring system always knows were a bag is and guarantees that no bag is forgotten. Another reason is, that a bag gets delayed, is that it has to wait until it reaches the security or other steps. With RFID you can identify all bags in the queue and prioritize the urgent ones.

Technical aspects at McCarran IATA member airlines approved the IATA Recommended Practice (RP) 1740C document (November 2005). This document recommends the use of ultra-high frequency (UHF) tags and readers, UHF means a range from 300 MHz to 3 GHz. Typically, UHF RFID tags must operate in three frequency ranges, 902-928 MHz (USA), 865.5-867.6 (EU) and 950-956 MHz (Japan). UHF tags and readers compliant with the ISO 18000-6C protocol (one international standard for the air interface protocol used in RFID systems for tagging goods within the supply chain.).

must be guaranteed, that critical parts of the system work correctly, even if a part of the primary equipment fails. Therefore, there are implemented four-antenna-arrays connected to multiple readers, connected in a configuration, that allows any of the readers to access the antennas in case of a readers failure. Certainly a redundant solution is needless, if it is not possible to separate the tags and identify the appropriate baggage, therefore more than 70 arrays have been installed into the system to secure the proper function of the security and sorting processes. Another challenge, that appears after the correct identification of working bag tags, was the identification of bags with a defective tag. However, FKI Logistex [7] has implemented a software/hardware/shielding solution.

At the moment, there are three airlines at McCarran's Terminal 1, which use RFID for Baggage tracking and airline workers attach smart labels onto the bar-codes sticking on the luggage. Each smart label contains an EPC (Electronic Product Code) class 0 inlay (a passive read only RFID microchip attached to an antenna and mounted on a substrate.). The data within tag contain three parts: a unique ID, an airline ID and a McCarran ID.

Outlook to the near future The next phase is set to begin early this year. In this deployment phase, the RFID inlays will be embedded in the labels. This will save manpower for the airlines. Also the airline tag will be removed. Instead, there will be one common database for all airlines, in which each bags unique ID is associated with the respective passenger's data and the airport ID. When another airports are tracking bags, they can link into this tracking system. For the second quarter of this year, the airport plans to expand the RFID system to all terminals, so that all 30 airlines will adopt the tracking system.

[7] http://fkilogistex.com/rfid/

In addition, McCarran works together with hotels in Las Vegas to develop an early check-in system. Under this system, a guest can check in at his hotel, his baggage will be tagged, security screened and send to the proper plane.

Even if IATA tries to speed up the use of RFID, in the foreseeable future there will be a parallel use of barcode systems and RFID systems. McCarran Airport will show that it is possible to run a only RFID system, which can do security screening and early baggage handling automatically. But it is not enough, one factor against a world-wide baggage tracking system is still the tagprice. Tags with memory must become cheaper to allow smart baggage, that knows its take-off airport, destination, intermediate landings, a lot of security information and of course information about the owner.

6 Smart Objects in Airplane Maintenance

Motivation Baggage management is not the only useful application for RFID in combination with airplanes. For Aircraft manufacturers, tagging airplane parts is a new option to reduce service costs. Boeing is the first manufacture to use this option, for the new 787 Dreamliner [8]. The suppliers have to place RFID tags on the parts before delivering them to Boeing. The production of the new airplane is planed to start in 2006 and the company's goal is to have their first dreamliner with tagged parts into service in 2008. A tag must be robust and durable, as it has to work under extreme conditions (temperature, pressure, humidity, vibration, attached to metal, ...), furthermore it should operate in the UHF band and should include 65 kilobytes of memory. There will be many different tags for different parts, some will be rigid, others flexible or they have to be housed in protective material and of course they may vary in size. Tags fulfilling all these requirements do not exist right now and will be developed in the next twelve months. The lifetime of such a tag will be about 20 year, and it will cost roughly 15$. A primary flight computer cost 400,000$, so it is much more reasonable to spend 15$ on a tag's life circle.

Currently Boeing is working with IT vendors on a software architecture, that supports RFID (The old software is based on manual entries and bar-code.) The Data stored in the RFID tag will not only include a unique ID, but maintenance and inspection data will also be saved. The encoded data in the tag will be synchronized in a database each time a mechanic services a part.

Maintenance, repair and overhaul (MRO) is a expensive progress, it is adds up to about 12% of the overall running-costs of an airplane and it underlies strict regulations for quality, security and documentation. It is not possible to say how Boeing will service planes in the future, but with tagging Dreamliner parts, they made big move towards the following scenario.

[8] http://www.Boeing.com/commercial/787family/index.html

6.1 Classical MRO process without Smart Items

The classical process takes place in an aircraft hangar, where different mechanics work together on one airplane. Each of the mechanics has his own toolbox, which includes a collection of typically used tools. If the mechanics need special tools, they can lend them at a central tool desk. The documentation is still stored partly on paper and partly digital on a computer. In addition there is a handbook library, containing maintenance instructions from the manufacturers and there are storage shelves containing spare parts

It is estimated, that a mechanic spends 15-20% of his time in searching for tools or documentation. This is a good starting point for making the process more efficient. Another costly part of the process is the tool management. A mechanic is responsible for the tools in his box and can also be held responsible for any damage caused by a tool, he has forgotten in a plain. Therefore any tool is manually marked with the identification number of the toolbox. In addition to that, the mechanics have to do routine completeness checks after each maintenance task. If a tool is missing, the aircraft is checked until the tool is found. Additional to that there is a base completeness test every week. For that two mechanics check each others toolboxes together for completeness and correctness and write a protocoll about it. If a mechanic wants to lend a special tool, he has to send a request to the service operator. A mechanic is allowed to check out 10 tools at one time. To guarantee this limit each mechanic has got ten metal tokens and his personal identification number is engraved on each token. When checking out a tool, the mechanic gives one of his tokens to the system operator. The operators three main tasks are. Checkout and finding out, weather the required tool is available, to returning and the following up of tools a mechanic has taken out.

Most weaknesses in the classic system are based on human errors and could be prevented by smart objects (in a smart infrastructure) assisting the mechanics, e.g. forgotten completeness checks, exchanged tools, misplaced tokens, missed documentations (checkouts and part servicing), irresponsible handling of the maintenance regulations, and so on.

6.2 MRO process with Smart Objects

Architecture The most important tool for the mechanics is their "Pervasive Device" (PD), the interface to the entire structure. The PD is also the connector between the real world objects and the digital world. It communicates with the system to execute a lot of tasks e.g. to access documentations of the parts, to get information about the workflow, to order tools for a special task, and so on. The communication between PD and the system could be realized with WLAN technology.

In addition, it has to communicate with the smart objects, primary to identify the objects (the objects can identify the mechanic too). For this RFID could be used. The intensity of the communication between the objects, the PD, other readers that inquire information and of course other objects, depends on the

"smartness" of the objects (this is shown below). A appropriate format to describe the exchanged data between parts of the infrastructure could be PML [9] an XML compliant description language.

If an object is not very smart, the infrastructure will read the identity and access a database to get all documentation and status information. Afterwards the system decides if a service is necessary (this could be possible for the parts and the tools) and sends all needed informations to the mechanic's PA. A real smart object has much more possibilities, if an object has got memory, the PD can get documentations, a list of all done services and who has made those services and at what time. With this information the PA (or the mechanic) can decide what to do directly. If an object has additionally sensors connected to it and a small processor, it is able to gain information about it's state from the sensors, or it knows, that it has to be serviced, because it has been in use for a certain time. These information can be read directly from the PA. If the object can send a signal, it can communicate with the managing system that it has to be exchanged or whatever. It may be also possible, that objects communicate among each other to get a more complex status report or to collect data at a specific point.

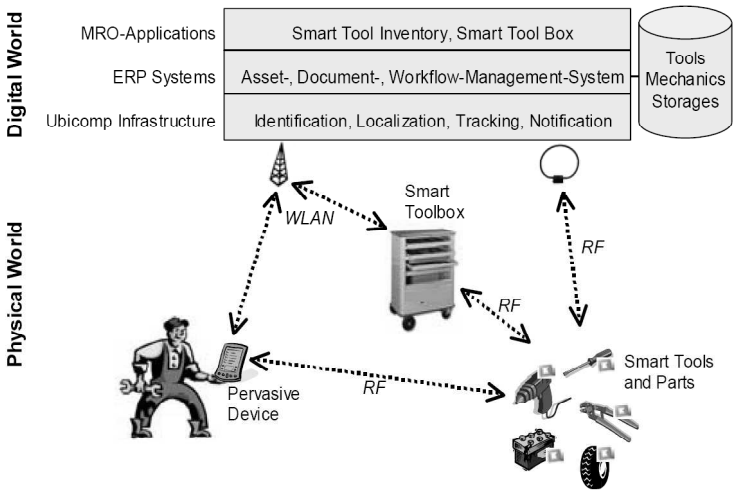

Fig. 5. MRO architecture with Smart Objects

Back on the architecture (Figure 5), on the physical side, we have the mentioned PA, the smart objects (tools, toolbox, parts) and a wireless communication-infrastructure composed of WLAN and RFID Tags/Readers. That allows us to

[9] http://xml.coverpages.org/pml-ons.html

identify, localize and track items. The UbiComp infrastructure is the base to realize all the functions in the layers above. In this solution any part of the real world has a virtual analog in the digital world and this virtual object offers services.

The next layer is the Enterprise Resource Planning (ERP) System. It provides a mechanic all needed information about the objects and he can access all needed documents for the MRO process. It is also possible to sign the documents with a digital signature. The Workflow Management System administers the MRO process, i.e. it guides the mechanic through the tasks of the MRO process (PD is the user interface) and it also automatically triggers checkout request for special tools and procurement of parts.

The last layer (MRO Application) contains two applications, the Smart Toolbox and the Smart Tool Inventory. Main task of the Smart Toolbox is to preform the completeness checks and notify the mechanic if any tool is missing or exchanged. The PD could receive a notification, that contains the location of the missing tool. Another function would be a controlling of the status of the tools by using sensors and monitoring the tools duration separately. If a tool is damaged or used too long, the mechanic would get a notification and in addition to that the box would send an order for a new one. The Smart Tool Inventory would realize self checkouts and returns of tools. Special tools could be ordered by the mechanic manually or automatically by PD. If a tool is not available, a reservation will be made or else the mechanic could identify himself to the Inventory and could get the inquired tool through a checkout box afterwards. Such a checkout box will handle the return process as well. The look up could be performed by a mechanic himself through his PD.

Typical Process Each mechanic has a Pervasive Device, that helps him to handle the service process. It is the only part of the architecture visible to him and it contains all needed information. At the beginning of the process, the PD informs him about the tasks, special tools needed and spare parts. After that he checks out the already reserved tools (after identifying himself) and takes the spare parts he needs. His PD verifies that he takes the right parts and receives customized information from the object. After obtaining the necessary tools and parts the PD guides him through the MRO tasks, it displays him all steps and gives him needed information from the handbooks. For each step he has to identify all parts that are involved in this step. The PD shows him the maintenance history and status reports. The mechanic has to describe the current status, which are written automatically on the part and/or into the database. After confirming the completion of a task an inspector gets a message and controls the part. If he is satisfied with the service he can digitally sign the part. At last the smart toolbox does a completeness check and the mechanic receives orders to bring back the special tools.

Improvements and Outlook Compared to the old structure, there are lots of improvements. Organizing and automation in all parts of the process, reduces

the delays during the process and they help to use resources more efficiently. Through that and the guiding process, many human errors can be avoided. The documentation becomes automatic and naturally the smart objects achieve a higher usability.

This scenario shows, that there are today useful applications/objects that can be realized. That Boeing forces the manufactures to tag their parts in the near future, indicates the request for smart objects, but as we have seen, it is a very long way from "dumb" objects to really smart ones.

7 Summary

We described very different applications with smart objects. Some are already implemented (like the baggage management at McCarran International Airport) and some are in research phase. From the very different range of applications all based on the same technology it is becoming obvious, that standards have to be defined. In case of the baggage management system and the attempt to expand it to other airports than the McCarran there are already existing standards. In other economical applications standards will be developed faster than in everyday applications since the economy has more power and interests to enforce standards.

As we described, smart objects are cost-efficient in economical applications. In everyday applications smart objects must be furthermore unobtrusive and accepted by the user. How many people would accept a full automated kitchen, that only allows to choose a recipe and the fridge automatically allocates the groceries or, if some are missing, generates a purchasing list and then cooks the meal automatically? In this scenario and in economical applications questions about security will arise. In everyday applications it must be ensured that data is protected. The baggage management system has to ensure that unauthorized persons don't get any information from the baggage. In applications like the airplane maintenance it is necessary to decide, which person or object is allowed to change information stored on tags, to avoid illegal manipulation of data. It is necessary to transfer existing security mechanisms from todays networks to interconnected smart objects.

Another challenge is how to handle the flood of information. Most of the existing infrastructures are overcharged with the masses of new data, so components with a higher bandwidth must be used. In addition to that applications and databases have to handle much more data too and a big part of the data has to be managed in real-time. To get all the data under control, efficient filters are required to differentiate between needed and unimportant information.

8 Conclusions

Today smart objects, as we defined them in this paper, don't exist. The technical development disallows the cheap and unobtrusive equipment of real world objects with sensors and processing units. With the development of the RFID technology

it is possible to integrate easily real world objects into the IT world. As we described they can turn into smart objects on the software layer. If the technical development progresses as fast as in the last years tags, sensors and processors will soon be cheaper and smaller. So it will be possible to convert many ordinary real world objects into smart objects on the physical layer.

References

1. Römer, Schoch, Mattern, Dübendörfer: Smart Identification Frameworks for Ubiquitous Computing Applications. In: Wireless Networks, Vol.10, No.6 (2004) 689-700
2. Langheinrich, Mattern, Römer, Vogt: First Steps Towards an Event-Based Infrastructure for Smart Things. Ubiquitous Computing Workshop, PACT 2000, Philadelphia (2000)
3. Srivastava, Muntz, Potkonjak: Smart Kindergarten: Sensor-based Wireless Networks for Smart Developmental Problem-solving Environments. In: ACM SIGMOBILE (2001)
4. Lampe, Strassner, Fleisch: A Ubiquitous Computing Environment for Aircraft Maintenance, ETH Zürich, University of St. Gallen (2004)
5. IATA: Recommended Practice 1740c - Radio Frequency Identification (RFID) specifications for interline baggage (2005)
6. FKI Logistex: Case Studies Series, Jacksonville International Airport (2005)
7. FKI Logistex: RFID for the Real World, Challenges and Opportunities for Airports (2005)
8. Andrew Price: Helping Bags Make Their Flights, `http://www.rfidjournal.com/article/articleview/1906/1/82/` (2005)
9. Mary Catherine O'Connor: McCarran Airport RFID System Takes Off, `http://www.rfidjournal.com/article/articleview/1949/1/1/` (2005)
10. Las Vegas Airport Bets on RFID, `http://www.rfidjournal.com/article/view/643` (2005)
11. Mary Catherine O'Connor: Boeing's Flight Plan for Dreamliner Tags, `http://www.rfidjournal.com/article/articleview/1956/1/1/` (2005)
12. Mary Catherine O'Connor: Boeing Wants Dreamliner Parts Tagged, `http://www.rfidjournal.com/article/articleview/1904/1/1/`
13. Mary Catherine O'Connor: Boeing Reveals More About Its Tag Plans, `http://www.rfidjournal.com/article/articleview/2011/1/1/` (2005)

RFID - New Application Scenarios

Healthcare Systems, Board/Card/RC Games and Human Activity Detection

Florian Dörr, Marco Heimberger, and Sebastian Kusch

Databases and Distributed Systems Group
Dept. of Computer Science, TU Darmstadt, Germany

Abstract. Radio Frequency Identification (RFID) gets more and more popular. In many areas it replaces the barcode technologies, since RFID is more robust and can store more information in the tag. The big benefit of RFID is the possibility to attach the tag to a product so that it gets uniquely identifiable, as long the tag is not destroyed or removed. However, RFID is not just a technology to replace barcodes in the Supply Chain Management, it can be used in much more branches. As smart keys to grant or deny access, for toll roads to track vehicles, for instance, and a lot of other applications are possible. This paper deals with future scenarios for Health Care Systems, Board/Card/RC Games and Human Activity Detection with regard to the possible usage of RFID technologies. As we will present, there are promising possible future applications out there, ranging from drug safety and support for elder healthcare to monitoring and locating tasks in rambling areas like theme parks. But also the gaming community will benefit from this technology where the real world melts with the digital one resulting in entirely new adventures.

1 Introduction

Radio Frequency Identification (RFID) is an identification method using devices called RFID tags or transponders for storing and retrieving data in a contactless way without intervisibility. An RFID tag is a small item that can be attached to any objects, like products, animals or humans. RFID is the generic term for the Transponder (called RFID chip -tag or -label) - where the data is stored - the Reader - the device that receives the data from the Transponder - and the Middleware that uses and controls the RFID system connecting it to the backend system. An RFID transponder usually consists of an antenna, a chip and - if the tag is active - a battery. The antenna enables it to communicate with an RFID reader whereas the chip stores the data. There are tree types of tags:

– **Passive Tags** have no internal power supply. The electrical current is induced in the antenna by the incoming radio frequency signal. It supplies the transponder with enough power to wake up and transmit a response. Since there is no onboard power supply the device can be quite small, so small that it can be embedded under the skin (the smallest devices commercially

available measured 0.4 mm 0.4 mm). Passive tags have a read distance range from about 10 mm up to about 1 meter. Due to their simplicity in design they are really cheap, about 5 - 10 Cents per Tag.

- **Semi-passive RFID tags** are quite similar to passive tags except for the addition of a very small battery. This small battery allows the tag to be powered, thus there is no necessity to collect power from the incoming signal.
- **Active RFID** tags have an internal power source, which is used to power all the chips on the transponder and generate the outgoing signal resulting in longer range and larger memories than in the passive case and they are able to store additional information sent by the transceiver. Most active tags have ranges of 10 meters, and a battery life of up to 10 years.

There is also a distinction in the used frequency, three ranges are recommended: Low frequency (LF, 30 - 500 kHz), High frequency (HF, 10 - 15 MHz) and Ultra high frequency (UHF, 850 - 950 MHz, 2,4 - 2,5 GHz, 5,8 GHz).

The EPC global organization is working on an international standard for the use of RFID and the Electronic Product Code (EPC) for the identification of any item in the supply chain for companies in any industry, anywhere in the world. With the power of the code stored in a RFID-tag each object/product can be uniquely identified as long as the tag is attached to the object. This is one big benefit compared to the bar code technology and there are even more advantages like support for longer distances, the possibility to read without intervisibility, active/passive as well as readable/writable tags, the ability to read several tags at once, automated technology, shared storing of data and faster read and write procedures.

The benefit for the supply chain management is an easy way to identify, locate and monitor goods as they travel through the supply chain between many companies. This way the accuracy of orders increases, the inventory handling cost are reduced, the inventory handling improves, fewer items are misplaced in warehouses and losses from theft can be reduced [1,2,3].

However, the supply chain management is not the only scope where the RFID technology might succeed, there are many more applications where RFID may play an important role. For example as smart keys to grant or deny access or for toll roads to track vehicles. The next chapters present future scenarios with regard to the usage of RFID technologies in the following fields: Healthcare Systems, Board/Card/RC Games and Human Activity Detection. Finally some of the major overall observations, trends and restrictions regarding the use of RFID technologies in future scenarios will be summarized in the conclusion section of this paper. In addition we would like to highlight at this point that in the next chapters we want to give an (inevitably incomplete) survey of possible future RFID applications, mainly in terms of current research projects. Not all of them are likely to turn into useful and well-accepted beneficial contributions one day.

2 Health Care

In contrast to "traditional RFID fields" like shipment and storage facility management applications in Health Care are relatively new and mainly still in a research stage. However, considering the complex demands and difficulties we are facing today in this area, RFID may be an important contribution to future development. Similar to other fields where this technology is applied (or will be applied one day) we can roughly divide these applications into three large domains: Identification, Tracking as well as Management and Optimization issues. Of course, these areas overlap, influence and rely on each other, but by means of this partition one may underline the main purpose of the application we are looking at.

It is important to note that we are speaking about a field with very high demands concerning correctness and dependability since there are not only economical values involved like in "traditional" applications (and it is not about gaming at all - an area we are dealing with in Section 3), it is about values up to human life. The following subsections present some application scenarios.

2.1 Labeling Embryos, Eggs and Sperm

In 2002, an English couple encountered an experience that may sound a bit droll, but only at first glance[4]: After a long and difficult IVF (in-vitro-fertilization) treatment their new-born twins turned out to be of mixed race, even if both parents were white. The sperm used for fertilization in the clinic had been mixed up, a more than annoying mistake.

In an attempt to prevent such cases in the future, the Human Fertilization and Embryology Authority (HFEA) which is responsible for these issues in the UK, considers labeling all embryos, eggs and sperm using a suitable technology like barcodes or - this is, where RFID gets important - electronic ID tags. For instance there might sound an alarm if the wrong eggs and sperms (i.e. with ID's that do not coincide) are brought too close together. Also the patients themselves may receive an unique ID in order to prevent a mishap as described above where a doctor attempts to implant a "wrong" embryo. Even if this application sounds relatively simple (we are talking about a system for mere identification) there is one important issue to be observed: Could the radio-waves involved in this technology harm the embryo? According to examinations where mouse embryos have been exposed to waves coming across in a system developed by Research Instruments, such tags can be run safely as long as they work at low frequencies and transmit only if they are activated by an external signal.

2.2 The Application of RFID in Drug Safety

Wu, Kuo and Diu from the Department Management of Information Systems of the Chung-Cheng University of Taiwan developed a pilot system aiming at enhancing the information flow in hospitals mainly in terms of patient and drug identification[5]. The system was designed to be compatible with (and extend

the abilities of) existing (in part already standardized) systems like the Hospital Information System (HIS), the Electronic Healthcare Record (EHR) and a drug storage management technology called Smart Medicine Cabinet (SMC).

According to Wu et al. these existing systems are often still lacking correctness and/or flexibility and do not interact with each other sufficiently, sometimes resulting in severe medical errors. As far as drug safety is concerned there are in their words two major types of such medical mistakes that are called Omission and Commission. The former means that the physician forgets some drugs or prescribes inappropriate dosage in the prescription, while the latter concerns about those drugs that are supplied to the wrong patients or at the wrong time.

Even if some hospitals already use systems like wristbands with barcodes for patient identification (and of course barcodes identifying drugs from the manufacturer as well) in order to reduce errors of the second kind, such technology only offers a fixed and limited amount of information to store whose content cannot be modified. For these reasons the RFID technology - without the shortcomings mentioned above - is said to become a powerful tool in drug safety and other fields of healthcare.

The system developed by Wu et al. is based on a 915 MHz passive read/write RFID tag and a barcode-co-system, as well as the HL/XML/SOAP data exchange standard inside the hospital. It is - according to Wu et al. - an evolutionary approach aiming at incrementally improving the system considering user feedback and the like.

From the physical point of view the system simply consists of a (conventional) bar code printed on the drug (packages) by the dispenser, 915 MHz read/write RFID hand rings worn by the patients, several RFID readers at several spots in the hospital and hand-held PDAs equipped with CF card readers and infrared readers for barcodes used by the medical staff. This way they are able to identify drugs, recognize patients, read out information about drug kind, quantity and possibly other precautions the patient should take as well as update the patient's HIS health record through 802.11.

From a logical viewpoint - however - the technology includes a more complex structure in terms of several subsystems.

The Medicine Tag Subsystem is mainly in charge of printing the tag, the Savant Management Subsystem deals with maintaining and revising the RFID technology involved (like the RFID rings for instance) and the Medical Component Subsystem needs to make sure that - in short - the right patient gets the right medicine and enforces relevant side-conditions if applicable. In addition there is the is the Medicine Entry and Exit Subsystem as well as the Patient Entry and Exit Subsystem tracking the drug entry and transfer and the patient's route of moving, respectively. For instance the former may propose a warning call if a reader device detects drugs entering limited area (see Fig 2).

Although Wu et al. do not provide any information about practical evaluations of their system at this point, they clearly express what they hope to achieve. According to them the core benefits are (among others):

– Right drugs in time avoiding taking drugs repeatedly by mistake

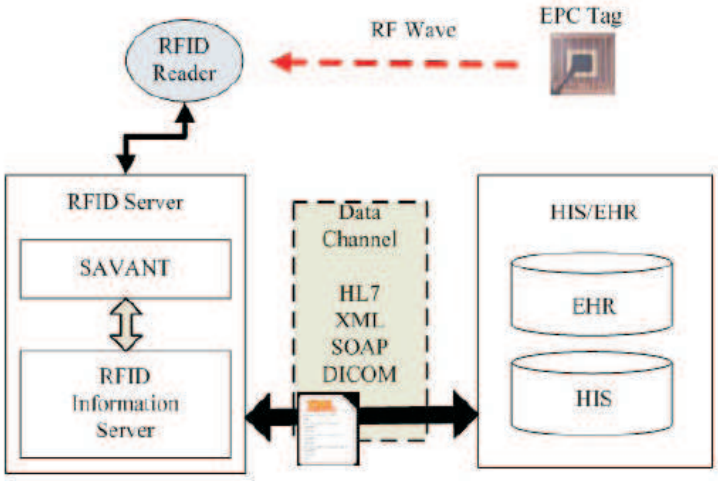

Fig. 1. System Architecture of Medicine Safety [5]

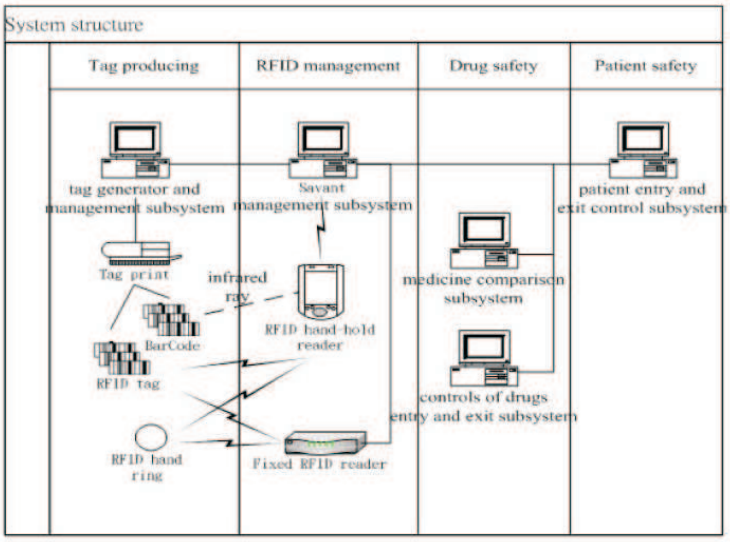

Fig. 2. System Structure of Medicine Safety [5]

- The ability to immediately grasp the amount of drugs of a certain kind in stock
- Highly dangerous drug control, e.g. in terms of high-temperature medicine of radioactivity
- Preventing pharmaceutical counterfeit

It might be worth mentioning that the FDA (Food and Drug Association) demands a general RFID tagging of drugs by 2007. Hence, pilot projects like this are likely to be an important contribution to future progress in health care and drug safety.

2.3 RFID and Sensor Networks

A fairly different approach for applying RFID technology in healthcare comes from Loc Ho et al., a team whose members work for Venturi Wireless, the San Jose State University and Fujitsu Lab of America, respectively [6].

They describe a prototype of an in-home elder healthcare system based on RFID technology and sensor networks. Their system aims at monitoring patients' medicine intake along with guiding them in their medication through a special GUI.

Sensor networks are (possibly very large in terms of the number of participants) distributed systems whose members - the nodes - themselves have only limited computational power each. However, communicating in an ad hoc and/or self-organizing style and equipped with the ability to read physical data from their environment (like temperature, for instance) they become a powerful tool e.g. for monitoring tasks with the necessity of instant data forwarding and processing in heterogeneous environments.

Hoc et al. propose a combined sensor network / RFID medicine monitoring system consisting of three "motes" (i.e. sensor nodes, in this case a sensor network platform called MSC Cricket by Crossbow [10]), namely the "Patient Mote", "the Base Station Mote" and the "Medicine Mote", an HF and an UHF (high frequency and ultra high frequency, respectively) RFID reader, a weight scale and a "base station" PC (See Fig 4).

The HF reader is in charge of tracking which medicine (bottles) - equipped with appropriate tags - are moved into, replaced or removed from its vicinity. Combining these events with the data from the scale the system tries to determine which amount of which medicine has been taken.

The UHF component on the other hand can be used to track the patient wearing a suitable tag. If the patient is in its vicinity the system may alert him to take the required medicine via acoustic signals and a special Patient GUI.

As to the tasks the several hardware components are meant to accomplish, note that in this application the sensor nodes are mainly used for communication (over relatively long distances, i.e. longer than the range of the readers), forwarding data from the readers to the control system, for instance.

In detail, the so-called Medicine Mote forwards data from the scale and from the HF reader whereas the Patient Mote communicates with the UHF reader, and the Base Station Mote provides message relay to the base station PC.

The software for the motes has been developed using TinyOS and the nesC language [11] and handles the communication with the readers and the base station along with sensor node specific issues like battery voltage management and the like.

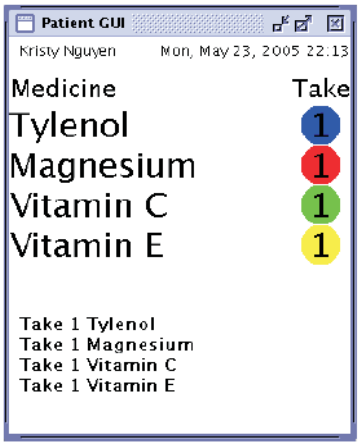

Fig. 3. Patient GUI [6]

The base station PC is programmed to process data received from the Base Station Mote. Written in Java it makes use of existing modules from TinyOS. It includes modules like a "Station GUI", the TinyOS reliable communication module for serial communication, modules for message decoding and MySQLServer for persistent database storaging.

Due to limited funding and to allow students to work on the project individually, a simulator was also developed for each hardware component. For instance, the RF and UHF RFID readers have been simulated using Java, emulating (in the latter case) the actual AWID UHF RFID reader protocol.

Also in this case we are dealing with an ongoing project. The proposed system is still in a research stage and - to our knowledge - has not been tested so far. However - apart from a few naive assumptions (How many patients do actually measure their medicine on a scale?) systems similar to the one described here will possibly become useful in-home assistants for elder people, provided that they are accepted as such.

2.4 RFID Wristbands for Surgical Patients

Chang-Gung Memorial Hospital has begun a pilot project involving RFID wristbands for its surgical patients [7]. Similar to the drug safety project described in Section 2.2, it stores relevant medical data (starting from aspects like patient

Fig. 4. Medicine Monitor System Prototype [6]

blood type for instance). The system is provided by Precision Dynamics Corp (PDC) and Hewlett Packard Taiwan Ltd. The readers - Hewlett Packard RFID Interrogators - have a range of about 10 cm and can be attached to an IPAQ HP pocket PC unit. Currently the hospital is using the system only in the surgical and recovery rooms - patient data can be accessed and/or recorded or updated - but according to HP the application might be extended to other hospital areas. Some data stored on the chip is read-only (such as the blood type) and cannot be altered whereas on the other hand hospital administrators are said to be able to encrypt other portions so that - e.g. in case of loss - third parties do not have unauthorized access to the data. Two U.S. hospitals - Massachusetts General Hospital in Boston and Georgetown University Hospital in Washington DC have similar projects on the way.

3 RFID in Board/Card/RC Games

The previous chapter presented some future scenarios and trends in the field of Health Care. Another field that might profit from the RFID technology in the future - where dependability is not a crucial factor - is the game industry. The following chapter examines in detail how RFID can be used to extend games. The general idea behind this field of applications is to build games using the RFID technology to fusion the real world with the digital one. In the virtual nature of computer games, the player plays against the computer or - in a multiplayer game - against/with one or more other players. The computer games take place

completely in the virtual world and there is no real social contact to other players. In a traditional game on the other hand players interact face-to-face using direct speech, gestures and mimics causing social situations. The goal behind applying RFID technology here is to build games that melt these two domains (the physical and the virtual one) to a game taking place in the real world but at the same time using the functionality of new technologies in order to interact with the virtual world. It turns out that RFID is in fact a suitable technology for interacting with the virtual world controlled by the computer. These types of games are referred to hybrid games in [12]. The following figure shows the general model of such games [12,13,20].

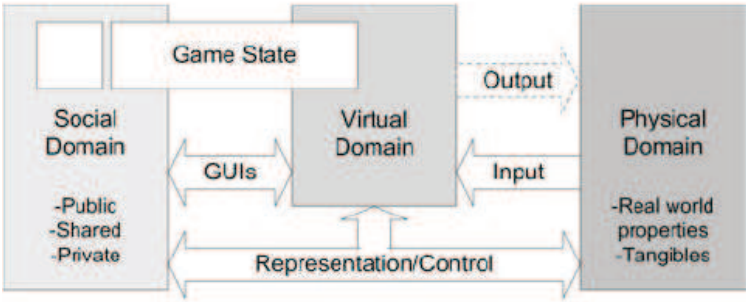

Fig. 5. Model of a Hybrid Game [12]

3.1 Board Games

One type of such games is a hybrid board game. Here, RFID technology can be used to realize an input device. Since the board game is normally quite small it suffices to use passive tags in the low frequency range. There is one RFID tag hidden in each relevant component of the game (such as a pawn, money markers, certain cards or other objects to keep track of). But we also need one or more appropriate RFID readers detecting the items by means of the tags. If these readers are placed into the game board, discrete positions and object identities can be detected. RFID is a very robust but slightly expensive technology for this purpose, the tags are really cheap but in general the readers are not. Nevertheless RFID is a suitable technology for these tasks as transponders can also store a few bytes of state information [12,13].

There are different tasks in a game that can be handled using RFID [14].

– **Remove object from position / Place object at position:** This is quite easy; as described above there are RFID readers on the board detecting the objects above them. If someone takes an object from a position the backend

system just has to know who was at the turn, so it can compute the new state of the game. Placing an object at a position is working just the other way round [14].

- **Passing object to a player:** This is essentially a special case of the task above, but it has to be handled differently since the objects are directly passed to another player. One possibility is that there is one reader for each player on the board, so the inventory of each player can be tracked. Another way to implement this task is to equip each player with a PDA along with an RFID reader keeping track of what items the player owns. This can be realized with a so called viewport - a hybrid interface. Viewport devices are special private interfaces with a GUI. The viewport consists of a PDA with the ability to communicate via WLAN detecting physical objects like playing pieces tagged with RFID transponders. Figure 6 (left) shows such a device displaying information about a tagged object that the viewport's owner has in its inventory. Figure 6 (right) shows the same viewport displaying information about an object belonging to another player [12,14].
- **Augmented Dice** This terms describes a dice with an RFID tag on each side that has to been thrown onto a dice surface containing an RFID reader. Each tag must be separated by a metal core so that only the tag on the bottom of the dice is detected [14]. In our view this might be hard to realize.

Fig. 6. Viewport Device used with tagged playing pieces [12]

Some implemented board games are presented in the following subsections.

Candyland "Candyland" is a hybrid gaming application for children (see Figure 7). "Candyland" represents the model of a small village, where physical

objects (citizens and houses) can be placed by the players. The physical objects and their positions are synchronized with their virtual counterparts using the RFID sensor interface integrated in the game board. The game logic runs a simple adventure game engine talking to the participants depending on how they move the playing pieces. "Candyland" aims at exploring how children make use of a hybrid game that combines digitized adventures and stories with interfaces they are familiar with [12].

Fig. 7. The "Candyland" Adventure Platform [12]

Fruit Salad "Fruit Salad" is a two-player board game making use of RFID technology. The board is built up to host plenty of removable "fruits", represented by tokens with images of the fruit and the corresponding RFID tag. The goal is to gather good combinations of individual fruit objects for one of the two real "salad bowls" integrated into the board. Each salad bowl is connected to an RFID reader telling the game logic the current progress of the fruit salad preparation. A real push-button is used to draw cards from a simulated deck which indicates a player's next turn. The board is composed of four round discs each of which is connected to a motor. A plastic apple with an accelerometer sensor inside is used during the game to control the rotation of the four board discs, thus changing the spatial arrangement of the available fruits. In total the game-technology consists of two push buttons, four motors, sixteen RFID tags, 2 RFID readers and the game logic running on a server. In addition, a computer screen or projector is used to display information about the game state like the players' overall scores or still missing fruits [15].

The Quest of the Amulet "The Quest of the Amulet" is a hybrid game that uses a physical game board as interaction medium. The board game consists of

8 * 8 fields, each with one landscape type like desert, hill or sea that is displayed through an image fixed on it. Each field has an RFID reader attached to it, so that it can detect a pawn in the game with an RFID label inside. The board continually updates the virtual representation. In the game there are two up to four players that are moving their pawns on the smart game board searching for shards of the broken amulet as well as for other items hidden on the board. Each pawn has a special character that causes advantages but also disadvantages compared to the others. The goal of the game is to find all shards of one arbitrary amulet. The one that gets this first, wins. There are different events that are triggered if a pawn is moved on a certain field and there are virtual characters moving invisibly over the game board disturbing the players figures. Since each character can just carry a limited amount of items, one have to put them down on the game board in order to pick them up later again.

In addition to the physical board game there is a screen displaying the public game information. Moreover each player has a separate private screen that shows the private game information. It is used to administrate the found items or to interact with a virtual character. The weather can change after each round causing different effects on different characters, for example in case of rain some characters cannot move as far as they normally can. The system also controls a lamp and a ventilator indicating the sun and the wind, as well as a sound system. To make sure that the game profits from the direct face-to-face interaction, trading off the items between players is one of the most important game processes [16].

Fig. 8. "The Quest of the Amulet" [16]

3.2 Card Games

Like in board games the RFID technology used for playing a hybrid card game is the same technology. That means passive RFID tags in low frequency and one or more RFID readers working at the same frequency. The only RFID card game we found is "Smart Playing Cards", but the technology behind it should be - for all card games based on RFID - the same. Here we describe the way the "Smart Playing Cards" is designed [18,19].

Smart Playing Cards "Smart Playing Cards" is a hybrid card game using the RFID technology communicating with the game system and is an enhancement of the card game of Whist, that will not be explained here. The developer chose the game of Whist because during the game there are never more than four cards on the table and they are easy for the used RFID antenna to detect. With today's readers it should be no problem to read much more tags at once lying on the table.

The hardware setup of the game is shown in Figure 10. It consists of an RFID reader, which is mounted underneath a table and connected to a PC, a set of PDAs, and a standard 52 card deck, where each card is joined with an RFID tag. Thus each card can be uniquely identified. The display connected to the PC shows game information common to all players, for example the current score. Each player can additionally use a PDA to obtain private information such as a rating of the current move [17].

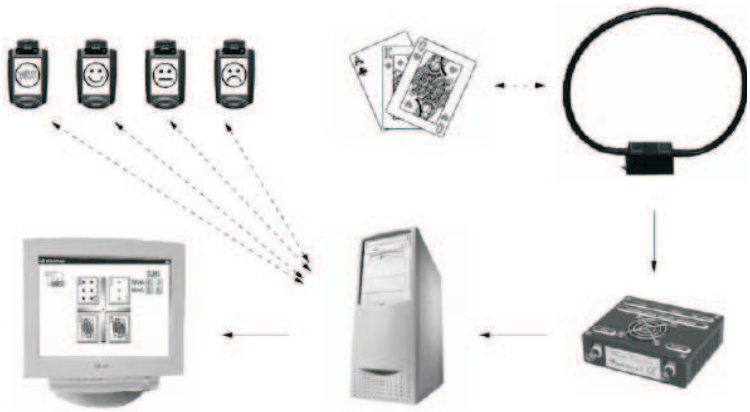

Fig. 9. "Smart Playing Cards" System Architecture [17]

In the first "Smart Playing Cards" application one big reader with an antenna of about 70 x 50cm in size was used. The detection range of such a reader is a sphere with a diameter close to the length of the antenna. This results in a quite

large area on the table where cards are detected, but players have to make sure that they keep the cards in their hands out of the detection range. Therefore it is better to use an array of smaller antennas. Tags located in overlapping regions are detected by more than one reader; so you can be sure that the card is lying on the table [17].

Smart Jigsaw Puzzle Assistant A jigsaw puzzle is not really a card game but it is closely related to it. Since the same RFID technology as for card games is used we describe it here in this chapter. The "Smart Jigsaw Puzzle Assistant" (JSPA) extends a normal puzzle game, so that it is possible to play the puzzle in different variations It also can help to find the next matching piece which means it solves the problem of searching a needle in the haystack. A miniature RFID tag is attached to the backside of each jigsaw piece. The RFID tags used are Hitachi m-chip inlets consisting of a tiny 0.4 mm x 0.4 mm m-chip with an external antenna of approximately 5 cm length. The RFID tags operate at a frequency of 2.45 GHz and have a 128-bit ROM for storing a unique ID. In addition there is a handheld scanner with an RFID reader inside to scan the puzzle pieces before adding them to the physical puzzle. Furthermore there are some game cards with an attached RFID tag for intuitive game control. During the game, one can read the tag of the corresponding card using the RFID handheld scanner in order to tell the system what one intends to do. If the reader recognizes a tag the functionality is delegated to the JSPA [20].

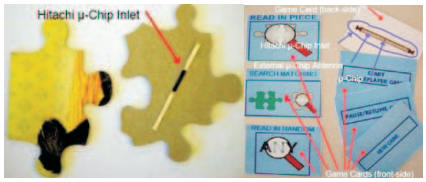

Fig. 10. A puzzle piece and game cards with RFID tags [20]

The SJPA supports a one-player mode and a competitive game mode for two players. In single player mode, the player chooses any piece to begin with. After that he or she tries to find and scan matching pieces as quickly as possible by placing the RFID reader on top of each new piece. If a new piece is matching, the player earns some points. Otherwise, if a scanned piece cannot be added to the previously combined pieces, the player looses points. If the player finds matching pieces within a certain time interval, he or she earns bonus points or may receive a joker. There is an "add random piece" joker and a "find matching piece" joker. Once the puzzle is completed, the value of the timer is subtracted from the player's score. If it turns out to be a new high score it is displayed in the SJPA's hall of fame. In multi-player mode, the SJPA randomly selects an initial

piece that has to be found and scanned by player one. Afterwards, the player is scanning and adding new jigsaw pieces to the puzzle. The SJPA keeps track of the players' scores and jokers, and displays the previously combined puzzle pieces on the screen [20].

3.3 Card Games

RC usually stands for 'remote controlled' but in the context of RFID it means 'radio controlled'. By definition most games introduced are radio controlled, so in the following, games not belonging to any other category (like card games for instance) will be referred to as 'RC Games'. Since in the RC Games' case one has to bridge more than just a few centimeters, the RFID technology involved needs to use a higher frequency range.

Pirates! Using the Physical World as a game board "Pirates!" is an RC game that uses PDAs connected to the WLAN and to an RFID sensor. Each player has a PDA as interface to the game's "virtuality", however, the game takes place in the real world - the so called game arena - with real objects. There are many physical objects in the game arena with an RFID tag attached to them.

The "Pirates!" environment is a fantasy setting where each player represents the captain of a ship. The tasks include facing a number of missions, exploring the islands to search for trading goods and treasures as well as fighting other players in sea battles. The ships, which have cannons and can harbour a number of crew members, allow the captains to sail the ocean and transport goods from islands in order to sell them at markets. If a ship sinks in battle, or if the crew is eaten by cannibals or lost while exploring islands, the game is over for the player concerned. Each island is different in terms of terrain, types of goods and valuables that can be found there as well as inhabitants. There is a free harbor where new crewmembers can be recruited. In addition one may have his ship repaired by spending the money earned by trading goods. Also located in the free harbor, the Viceroy's office charges the captains with new missions. Captains, successfully completing missions, are awarded with higher ranks by the Viceroy, and equipped with bigger and stronger ships [18].

The RFID technology used is operating at the unregulated ISM band. Since there is the need to communicate bi-directionally, each object and handheld device is equipped with an RFID tag as well as with an RFID reader. Therefore all objects and PDAs are listening to other RFID sensors, and each RFID tag is responding with his unique ID. When a sensor mounted on a PDA device detects a signal from another device, a notification is sent to the game engine (on the game server) via the WLAN connection.

Using this technique it is possible to determine the physical whereabouts of players in the game, relying on the sensors, which tag physical locations and other handheld devices. The RFID sensors placed at a number of fixed locations in the game arena are marking virtual islands in the game arena. The sensors

attached to each handheld computer are used to detect when the players are in the vicinity of islands (player-to-place proximity), or other players (player-to-player proximity). This enables some of the game mechanics and forces the players to physically navigate the game arena in order to explore the virtual game environment. [18]

Tagaboo "Tagaboo" is a children's game based on wearable RFID technology. Tagaboo combines traditional athletic children's games with physical objects equipped with RFID tags inside that are bound to different sounds and behaviors. These objects (tokens) are hidden in pockets placed on a wearable vest. While one or more children wear such vests, children may "seek" for tokens using a special glove, with an embedded RFID reader and computing capability, e.g. using a handheld device. "Tagaboo" is based on the game "hide-and-seek", "Catching" and "Memory". If one touches a pocket (with the glove) holding a token inside, a special sound is played and the correlating points are added in the handheld device running the game engine. If a child touches a pocket which it already has touched before, a bad sound will appear and he or she will loose points. There are a lot of possible game varieties. For example, like in Figure 12 on the left-hand side, there are one or more catchers wearing the glove and there are one or more escapers wearing the vest with the pockets on it. In some pockets there are special objects inside and other pockets are empty. The catchers have to collect as many different objects as possible within a fixed time period. The one to get the most points is the winner. In another variant, shown in Figure 12 on the right-hand side, each player has a wearable vest along with a glove. He has to catch objects from other children and at the same time be aware of getting touched by the other players.

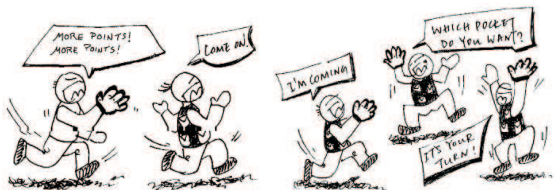

Fig. 11. "Tag boo" with Catchers and Escapers vs. each child with a glove and a vest mode [19]

The RFID technology involved here is based on passive tags that are small coin-shaped Philips HiTag RFID tags, each including a unique identification number. The tags were sensed by a small (23 cm) RFID reader. If one touches a pocket, only the tag within this pocket is meant to respond. Thus, the radio frequency technology used has to have a very small range. [19]

Casinos bet on RFID Technology Also Casinos make use of the RFID technology. That is not a game but it is related to the environment of games. Casinos all over the world are interested in RFID technology. They plan to install a tag into each chip and one or more reader into each table. When the dealer closes all betting, the RFID technology could register the wagers, thereby unmasking players who try to add or to remove chips surreptitiously. The RFID system could also record activities at a table for bookkeeping purposes and may detect thefts. The only difficulty yet is that RFID readers in the game table require seven seconds to read 100 chips, which is too slow for fast-moving games such as baccarat, pai-gow poker, or roulette. However, faster RFID technology will probably solve this problem in the future [21]. The idea of detecting thefts mentioned here is already an application of Human Activity Detection, a field we are going to deal with in the following section.

4 Human Activity Detection

So far some future scenarios using RFID technologies in the fields of Health Care and Gaming have been presented. Before summarizing the major trends and restrictions in the conclusion section, the following chapter deals with one more related topic, namely the human activity detection, looking in detail at how this may be realized in the future by means of RFID technologies. Objective of human activity detection research is to infer people's current behavior and their actions to use this information as an implicit input for computer systems. The ability to infer what a person is doing or attempting to do could be very useful in many ubiquitous computing scenarios. In the past the techniques for human activity detection were based on direct observation of people and their behavior by means of cameras, contact switches and worn accelerometers. A recent avenue, which seems to be very promising [29], is to supplement direct observation with an indirect approach, inferring a person's actions by their effect on the environment. One way to do this is by observing the objects a person interacts with. Researchers have applied different techniques to human activity detection. Active sensor beacons [23] are one of these techniques. They provide accurate object identification but require batteries, making them impractical for long-term dense deployment. A modern technique that might be useful for human activity detection is RFID. The RFID tags potentially have the same object-identification accuracy as active beacons, with the advantage of being battery-free (passive tags). However, unlike sensor beacons, they are unable to detect motion [25].

Talking about the use of RFID technology for human activity detection there are basically three different approaches. The first approach is based on people wearing RFID readers, which read the RFID tags of near objects. The second possibility is focused on RFID tagged objects, which are observed and used to infer the activity of a person interacting with these objects. The third alternative is based on people wearing RFID tags. Of course the three opportunities may be combined in different scenarios. The following sections discuss each of the three

approaches and present some illustrating examples. Finally, a short overview of some more sophisticated scenarios and related topics is given.

4.1 People wearing RFID Readers

One way to approach human activity detection is by equipping people with wearable RFID readers and some objects in their environment with (passive) RFID tags. Whenever a person comes close enough to a tagged object the reader activates this tag and receives its data. The information about who is using particular objects can be used in multiple ways by attached systems. Many activities involve the manipulation of particular physical objects. Cooking, for example, involves pans and dishes being moved. Therefore a particular activity could be recognized from a time-sequence of object touches.

iBracelet The iBracelet is a wrist-worn short-range RFID reader that detects object use via hand proximity. The iBracelet system uses just one battery to power its reader and yields information about who is using particular objects. The read range has to be large enough (10-15 cm), as the wrist-worn antenna is typically not in direct contact with the tags. However, the wearable-reader approach still involves some open questions about basic feasibility. It depends on the application scenario what combination of size, aesthetics, and battery lifetime will satisfy a consumer's needs if that is even possible. The iBracelet appears promising for industrial or enterprise-context human activity inference applications in which a wearable reader is not a burdensome requirement [25].

Real World Bookmarks A wearable tag reader similar to the iBracelet has been used for a case study to explore implicit human computer interaction using RFIDs [34]. A wearable computer is connected via a serial line to the reader module. While a RFID tagged object is nearby, the reader sends the unique object ID over the serial line to the wearable computer. The system's software consists of three parts: a module listening on the serial port, a web browser component, and a mapping table. The software maps a received RFID to a URL on the WWW according to the mapping table. Then the web browser is called with this URL. Physical objects often have a specific meaning to the user or are involved in a particular activity. When their ID is associated with an URL, objects can serve as real-world bookmarks. Here are some application examples that employ object/URL mappings:

- use objects to trigger applications: pick up pen ¿ open editor by calling a URL
- use objects as bookmarks to information: can of beans ¿ suggest a recipe
- use personal objects to access individual information: credit card ¿ show user's bank balance [34]

GETA Sandals Within the GETA project [27] RFID technology has been used to support a footprint-based indoor location system on traditional Japanese GETA sandals. The footprint location system works by measuring and tracking the displacement vectors along a trial of footprints. Each displacement vector is formed by drawing a line between each pair of footprints. The position of a user can be calculated by summing up the current and all previous displacement vectors. The vector information is derived from infrared readers and transmitters placed on the GETA sandals triggered by a pressure sensor. However, the footprint-based method suffers from accumulative error over distance traveled. To address this issue, it is combined with a light RFID infrastructure to correct its positioning error over some long distance traveled. Therefore a number of passive RFID tags with known location coordinates are utilized in the environment and a small RFID reader is placed under a GETA sandal to read these RFID tags. When a user walks on top of a location-aware RFID tag, the known location coordinate of that RFID tag is used instead of the calculated footprint location. Encountering an RFID tag has the same effect as resetting the accumulated error to zero [27].

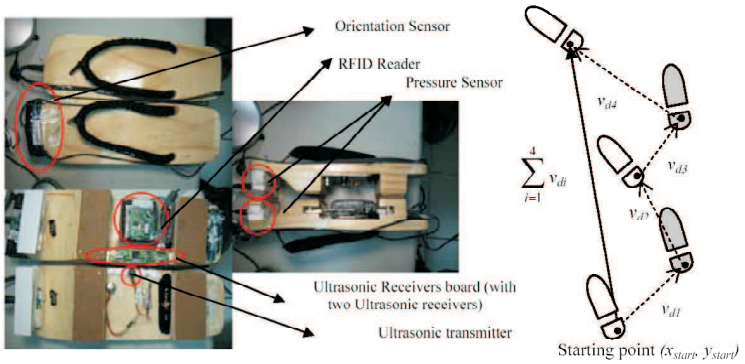

Fig. 12. Prototype of the GETA Sandals [27]

This scenario shows one way RFID technology may be used to locate a person. If it is not necessary to locate a person very precisely, one could use RFID technology as described but without any additional sensors. In addition of the current location of the person, the possible destination of the person moving may be derived by the temporal order in which the location-aware RFID tags are read. This information may be used to turn lights on or off, adjust room temperatures and so on as a person is moving towards a specific location. Localization with RFID technology is still a research topic and there are some interesting papers [28] available.

4.2 Observation of RFID tagged Objects

Another possibility to do human activity detection not requiring human-worn RFID readers is to observe RFID tagged objects and try to infer the activity of a person interacting with these objects. To observe a persons interaction with an object it would be very useful to be able to detect the object's motion. Unfortunately RFID tags are not able to detect motion but they may be augmented with sensors that are. Under these conditions human activity may be tracked by detecting the motion of different objects over time and inferring patterns for corresponding activities. If an activity reoccurs these patterns can be used to recognize it. Neural networks may be used to realize this idea. In a training phase the network has to learn the patterns for different activities to be able to recognize these activities again. Imagine a person getting up in the morning. After entering the bathroom, the person interacts with some objects like the toothbrush, a towel, hairspray, a lipstick and so on. The objects moved will be more or less the same every morning. Sometimes the person does not use a lipstick or uses the objects in another order than the day before but at least four out of the objects will be used within a certain time interval every morning. An attached system is able to learn to recognize this activity and use this information to prepare a cup of coffee for example. There are many possible application scenarios where the information about objects being used yields to the activity of a person. The knowledge of a person's activity can be used as a very powerful implicit input to any attached system.

WISP The Wireless Identification and Sensing Platform (WISP) is a family of long-range RFID tags augmented with sensors that detect object motion [25]. They use long-range motion-sensitive tags read by fixed infrastructure. WISPs deliver motion detection capabilities in the same battery-free form factor as RFID tags using line-powered readers. A WISP consists of passive RFID tags augmented beyond the basic identification capability of ordinary RFID. Like ordinary passive RFID tags, WISPs do not have an on-board power source but they get their power from RFID readers. There are two kinds of WISPs, the alpha- and the pi-WISP. The alpha-WISP is able to detect object motion along a single axis by selectively enable or disable a first or second RFID tag. Ordinary RFID tags consist of a single chip mounted on a single antenna. The alpha-WISP consists of an antenna with two chips and two mercury switches (one-bit accelerometer and modulating element). If the object is in its rest configuration, the first ID chip is connected to the antenna and the first ID is detected by the reader. If the object is tilted, the first chip is disabled and the second enabled, so the second ID is detected by the reader. Reading either of a WISPs IDs indicates that a physical object is present in the reader's range of view. If both ID values show up within a small time interval this indicates that the object is also moving. The three-axis sensor pi-WISP is more complex and allows detecting object motion along three axes. It consists of a power-harvesting circuit, an ultra-low-power micro-controller, a three-axis-by-one-bit mercury-switch-based accelerometer and an electronically controlled 2:1 multiplexer that allows the

micro-controller to connect a first or second RFID integrated circuit to the antenna [25].

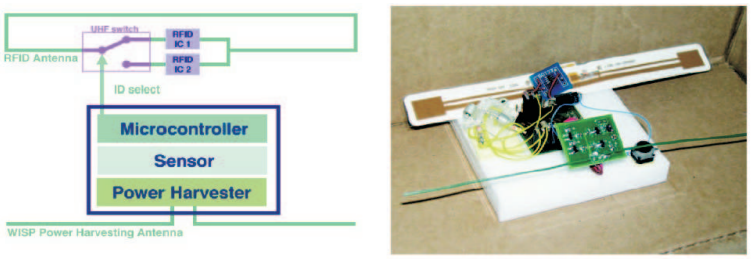

Fig. 13. Block Diagram and photograph of the pi-WISP [25]

Information about object movement can be encoded by a choice of RFID tag ID values over time (ID modulation) so the system is able to recognize if and how an object is moving. This motion information can be used for a WISP-based activity detection process.

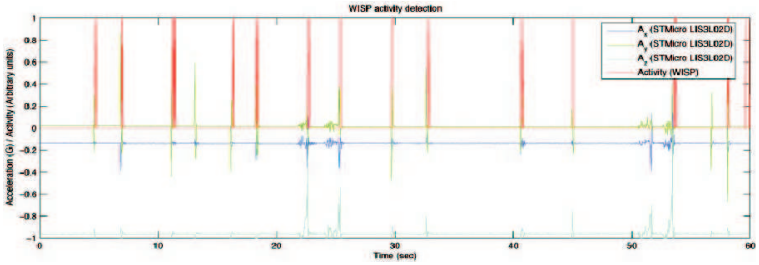

Fig. 14. WISP Activity Detection [25]

The WISP based approach not only allows to detect if an object is moving but also how it is moving. This may simplify inferring human activities from objects being moved. Imagine a ball equipped with WISPs (assuming an according size of the WISPs). It might be possible to distinguish if the ball is kicked (indicating people playing football) or used to play volleyball.

4.3 People wearing RFID Tags

Instead of equipping people with wearable readers that read RFID tagged objects placed in their environment there is also the opposite possibility based on people

wearing RFID tags, which are read by readers installed in their environment. One can realize scenarios similar to the ones described so far using this approach. The only difference is that the readers are placed in the environment and therefore the attached system dealing with the information is usually apart from the people wearing the RFID tags. Imagine RFID tags like the WISP that can be worn by humans. Instead of observing tagged objects trying to infer the activity of persons interacting with these objects you can also directly observe the RFID tagged people and try to infer their current activity by their movements, although the sending range of the tags must be reasonably large.

The approach where humans wear RFID tags is mainly used for locating people or animals and for tracking their movements. The RFID tags can easily be integrated into clothes or passports for example. There is even the possibility to implant RFID tags under the skin [22, 31]. The idea for roughly locating people or pets wearing RFID tags is very straightforward. There are several RFID readers installed at known locations and every time a person or pet wearing a tag comes close to one of these readers the corresponding ID is read so an attached system knows the current location. Furthermore the possible destination of the person moving might be inferred by a sequence of read events over time. Imagine a theme park with RFID readers installed at key locations and all visitors wearing RFID tags. If a movement straight towards the exit is recognized the system can infer that the corresponding person intends to leave the park and may take further actions like displaying a goodbye message on a screen for example. There are many possible scenarios for this kind of human activity detection based on locating people and tracking their movements.

Locating Children According to ZDNet Asia [33] the school authorities in the Japanese city of Osaka have decided to tag the school kids with RFID chips. The chips will be put onto the kids' schoolbags, nametags or clothing in a Wakayama prefecture school. The tags will be read by readers installed in school gates and other key locations to track the kids' movements. Denmark's Legoland introduced a similar scheme to stop young children going astray [33].

4.4 A more Sophisticated Scenario

So far three different approaches to human activity detection, which may be combined, have been introduced and illustrated by some examples. This final section sketches a more sophisticated scenario for human activity detection based on RFID technology.

Using Spatio-Temporal Constraints for Human Activity Tracking User activity assistant systems that take the user's context into account typically consider the spatial relationships between humans and objects in the environment. This spatial information is an important aspect of the user's context and activity. However, temporal information is an important aspect of the user's activity as well. By ascertaining and analyzing both the spatial and temporal relationships

between the user and objects, it is possible to support the user's activities in a more sophisticated manner [32]. The use of Hidden Markov Models has been proposed to recognize a user's state from time-series information [35, 24, 26] but, to recognize the state of a user performing actions in real-world situations, it is necessary to deal with time scales ranging from short-term transitions to long-term changes that may take place over several hours. To adapt flexibly to the time scale of the user's state, it is necessary to be able to change the time axis resolution adaptively according to different user's activities.

A paper proposed by Y. Isoda, S. Kurakake and H. Nakano [32] describes the use of RFID tags and floor-mounted weight sensors, installed inside an experimental house, to detect the spatio-temporal relationship between a human user and various objects, and discusses a method for representing the user's state based on information obtained from these devices with multi-resolution as spatio-temporal attributes. The paper proposes a user activity assistance system that performs robust state decision by learning which attributes are valid for discriminating between the user's states based on information obtained from these sensors. A user completes tasks by performing specific state transitions following a series of procedures. However, the states associated with specific tasks do not always occur consecutively and there may be tasks for which there is no inherent sequential relationship of states. Therefore it is necessary to recognize states of discontinuous time series to support the user in his activities. For the case study described in the paper, some task models consisting of a set of user states for each task were prepared and adapted to a user's state series that could be detected by using ubiquitous sensor information. The system proposed contains a state recognition module, where sensor information is transformed to a spatio-temporal representation of a user's state. A user's state is discriminated by a decision tree constructed in a teaching phase. Attributes that are valid for discriminating between user's states are learned as nodes of the decision tree. The state recognition module provides a series of user's states to a user assistance module, which is also part of the proposed system. The user assistance module executes user assistance by matching the series of user states to a task model representing a specific activity.

Within the study [32], the attributes representing a user's state are derived from information obtained from RFID tags carried by the users and attached to objects. The RFID tag information detected by each RFID tag reader is collected for each user. In addition to the information on the presence or absence of objects in each user's vicinity, the temporal continuity of presence of these objects is also incorporated as attributes of the user's state. The user's state is represented by attributes that include information on how long each object has existed in the user's vicinity due to the user's movements and whether or not the objects in question are carried around by the user. The overall set of attributes describes the state of a user in relation to these objects at time t. The user's vicinity corresponds to the detection ranges of the tag readers that detect the RFID tag carried by the user, so all the objects detected by the same tag readers that detect the tag carried by the user are in the user's vicinity. This

way, the user's state is represented by attributes expressing which objects are in the user's vicinity, and if so, for how long. In addition to the relative positional relationships between the user and objects as detected by the RFID tags, the user's absolute position (derived by the floor-mounted weight sensors) is also used as attributes representing the user state.

Fig. 16 illustrates the use of RFID technology in the scenario described above. It shows the RFID tag information detected by each RFID reader collected for each user (left) and the attributes relating to the user's objects at times t1 and t2 (right).

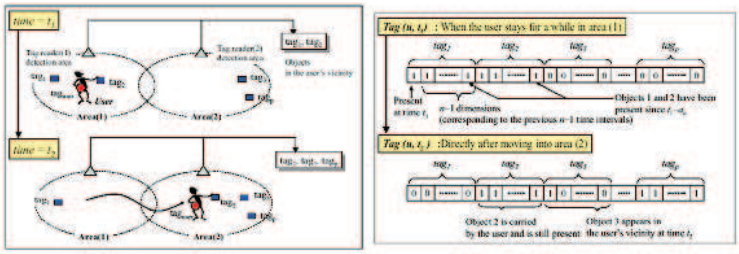

Fig. 15. Changes of RFID Tags associated with Movement of the User [32]

To discriminate between the diverse states of users in everyday activities, it is difficult to determine what sort of characteristics should be extracted from the sensor information and how the model should be constructed to distinguish successfully between each of these states. One possible approach presented in the study [32] is to employ a learning-based behavior model in which information obtained from RFID tags and sensors is directly mapped to classes of states to be discriminated. A learning algorithm (C4.5) [30] is used to learn the attributes that are valid for discriminating between the classes of states and to construct the decision tree. The decision tree discriminates between different state classes by applying the entire set of attributes obtained from RFID tags and sensors at fixed time intervals. The result is a series of state classes, which can be used to identify a corresponding prepared task model consisting of a set of user states describing a specific activity. A model of each task is pre-registered as a module describing the task start- and execution conditions, the task execution state, the user support methods, and the task completion conditions. Each of these task modules is executed separately to provide users with appropriate support even when performing different tasks in parallel. Imagine a user being involved in the preparation of food in the kitchen but has to leave the kitchen temporarily to answer the phone and returns after an interval. The user support module could be used to remind the user of the state that had been reached before the user left the room. This example shows that human activity detection scenarios may easily become very complex [32].

5 Conclusions

After examining the three fields Healthcare, Games and Human Activity Detection with regard to the usage of RFID technology we will now try to present the overall observations and draw some conclusions. The scenarios presented show that RFID technology is a technology with a promising future, even if there are still some problems and limitations that need to be solved.

Above all there is the need for small tags but especially for smaller readers. In the field of gaming, small tags are necessary for cards, puzzle pieces (section 3.2) or counters. There is also a demand for smaller readers that can be integrated into areas of board games (section 3.1). Regarding Healthcare the wristband scenario (section 2.4) indicates the requirement for smaller tags as well, so the wristband may be built very small and does not handicap the patients. In the human activity scenarios describing the GETA sandals and the iBracelet (section 4.1) the need for smaller readers is obvious. Of course there are quite small tags available but not for a price that allows an unlimited extensive integration. In a card game with 52 cards like the smart playing cards presented in section 3.2, very small tags need to be attached to each card. The same applies to puzzles like the smart jigsaw puzzle in section 3.2 with 1000 smart pieces and of course to healthcare systems since each test tube, blood bottle and all patients may be equipped with tags or readers. If you consider only one tag, a price of about 20 Cent is no object, but if you have to integrate thousands of tags in a small application it gets relevant. The matter of size becomes even more problematic as the RFID tags and readers are combined with other technologies leading to enriched functionalities but also to larger sizes as the motion sensitive WISPs described in section 4.2 show.

Another aspect the three observed fields have in common is the trend of combining RFID with other technologies to achieve enriched functionality. This is essential since RFID evolves its real power only in combination with other technologies allowing more than just basic RFID functionality. In the field of Healthcare, for example, temperature- or radiance sensors can be useful (section 2.2). As to Human Activity Detection, additional pressure sensors are used in the GETA sandals scenario (section 4.1), and for the WIPS scenario, RFID has been combined with motion sensors (section 4.2). Regarding Games, RFID technology is used in "The quest of the amulet" to trigger the control of a lamp and a ventilator. In the "Fruit Salad" game, RFID is used together with a control system that monitors engines and buttons. Of course most of the presented games and scenarios are based on WLAN technology being combined with RFID. The combination of RFID with other technologies allows more complex applications.

In short, many future scenarios require smaller and cheaper RFID tags and readers to facilitate an extensive integration. Moreover RFID on its own only offers a basic functionality, but combined with other technologies it becomes applicable in manifold future scenarios like the ones we described here. In addition, we are confident that there will be even more new and complex RFID scenarios soon that overcome today's shortcomings getting more and more relevant in everyday life.

6 References

1. Tim Kröner: http://www.rfid-journal.de/
2. Wikipedia-RFID: http://de.wikipedia.org/wiki/Rfid, http://en.wikipedia.org/wiki/Rfid
3. Dr. Mariano Cilia: AutoID and Web Presence, Part 8 of the Lecture Client/Server, Middleware and EAI, Department: Databases and Distributed Systems, Darmstadt University of Technology (2005)
4. Shaoni Bhattacharya, April 2005: http://www.newscientist.com/
5. Fan Wu, Frank Kuo, Lie-Wei Liu: The Application of RFID in Drug Safety of Inpatient Nursing Healthcare, ICE'05, August 15-17, 2005, Xi'an, China
6. Loc Ho, Melody Moh, Zachary Walker, Takeo Hamada, Ching-Fong Su: A Prototype on RFID and Sensor Networks for Elder Healthcare: Progress Report, SIGCOMM'05 Workshops, August 22-26, 2005, Philadelphia, PA, USA
7. Claire Swedberg, July 2005: http://www.rfidjournal.com/
8. WHO, http://www.who.int/en/
9. Taiwan Health Reform Foundation, http://www.thrf.org.tw/
10. Crossbow Inc., http://xbow.com/
11. TinyOS, "TinyOS Community Forum", http://www.tinyos.net/
12. Carsten Magerkurt, Timo Engelke, Maral Memisoglu: Augmenting the Virtual Domain with Physical and Social Elements. ACM Press New York, Computers in Entertainment, Volume 2 , Issue 4, New York (October 2004)
13. Sus Lundgren: Joining Bits and Pieces - How to make Entirely New Board Games using Embedded Computer Technology. MSc Thesis in Interaction Design, Gteborg (2002)
14. Daniel Eriksson, Johan Peitz, Staffan Björk: ENHANCING BOARD GAMES WITH ELECTRONICS. Interactive Institute Game Studio, 3rd International Conference on Pervasive Computing (2005)
15. Bernhard Jung, Andreas Schrader, Darren V. Carlson: Tangible Interfaces for Pervasive Gaming. ISNM - International School of New Media, Lübeck, 3rd International Conference on Pervasive Computing (2005)
16. Carsten Magerkurth, Maral Memisoglu, Wolfgang Hinrich: Entwurf und Umsetzung Hybrider Spielanwendungen. Mensch und Computer 2005: Kunst und Wissenschaft - Grenzüberschreitungen der interaktiven ART. München: Oldenbourg Verlag (2005)
17. Kay Römer, Svetlana Domnitcheva: Smart Playing Cards - A Ubiquitous Computing Game. Department of Computer Science ETH Zürich, Springer-Verlag London, Personal and Ubiquitous Computing, Volume 6, Issue 5-6, London, (December 2002)
18. Staffan Björk, Jennica Falk, Rebecca Hansson, Peter Ljungstrand: Pirates! - Using the Physical World as a Game Board. PLAY research studio, Interactive Institute c/o Viktoria Institute, Gteborg, In Proceedings of Interact'01, Tokyo (2001)
19. Miriam Konkel, Vivian Leung, Brygg Ullmer, Catherine Hu: Tagaboo: a collaborative children's game based upon wearable RFID technology. Pers. Ubiquit. Comput., Springer-Verlag London (2004)
20. Jürgen Bohn: The Smart Jigsaw Puzzle Assistant - Using RFID Technology for Building Augmented Real-World Games. Institute for Pervasive Computing, ETH Zürich (2004)
21. Casinos Bet on RFID Technology. Computer published by IEEE Computer Society

Computer April 2005 Vol. 38 Issue 4, p.25, (April 2005)
22. Digital Angel Corporation: http://www.digitalangelcorp.com/
23. E. Munguia Tapia, N. Marmasse, S. Intille, K. Larson: Wireless portable sensors for studying behavior. Extended Abstracts of the Sixth International Conference on Ubiquitous Computing. Nottingham, England, Sept. 7-10 (2004)
24. Henry Kautz: Understanding Human Behavior from Sensor Data. ICAPS'05 invited talk. http://icaps05.uni-ulm.de/documents/invitedTalks/ICAPS05-Kautz.pdf
25. Joshua R. Smith, Kenneth P. Fishkin, Bing Jiang, Alexander Mamishev, Matthai Philipose, Adam D. Reah, Sumit Roy, Kishore Sundara-Rajan: RFID-based Techiques for Human-Activity Detection. Journal of Communications of the ACM, September, Volume 48, Number 9 (2005)
26. J. Yamato, J. Ohya, K. Ishii: Recognizing Human Action in Time-Sequential Images using Hidden Markov Models. Proceedings of CVPR'92, (1992), pp.379-387
27. Kenji Okuda, Shun-yuan Yeh, Chon-in Wu, Keng-hao Chang, Hao-hua Chu: The GETA Sandals: A Footprint Location Tracking System. Department of Computer Science and Information Engineering, Institute of Networking and Multimedia, National Taiwan University (2005)
28. Matthai Philipose, Kenneth P. Fishkin, Dieter Fox, Dirk Hahnel, Wolfram Burgard: Mapping and Localization with RFID Technology. Intel Research, IRS-TR-03-014 (2003)
29. Matthai Philipose, Kenneth P. Fishkin, D. Patterson, M. Perkowitz, D. Hahnel, D. Fox, H. Kautz: Inferring activities from interactions with objects. IEEE Pervasive Computing Magazine 3, 4 (Oct.-Dec. 2004), 50-57
30. R. Quinlan: C4.5 - Programs For Machine Learning, Morgan Kaufmann Publishers Inc. (1993)
31. VeriChip Corporation: http://www.verchipcorp.com/
32. Yoshinori Isoda, Shoji Kurakake, Hirotaka Nakano: Ubiquitous Sensors based Human Behavior Modeling and Recognition using a Spatio-Temporal Representation of User States. Proceedings of the 18th International Conference on Advanced Information Networking and Application (AINA'04), IEEE Publication 0-7695-2051-0/04 (2004)
33. ZDNet Asia: http://www.zdnetasia.com/news/hardware/0,39042972,39186467,00.htm
34. Albrecht Schmidt, Hans-W. Gellersen, Christian Merz: Enabling Implicit Human Computer Interaction - A Wearable RFID-Tag Reader. IEEE Publication 0-7695-0795-6/00 (2000)
35. B. Clarkson, A. Pentland: Predicting Daily Behavior via Wearable Sensors. TR540 (2001)

Author Index