Universidad de Oviedo

ESCUELA POLITÉCNICA DE INGENIERÍA DE GIJÓN.

GRADO EN INGENIERÍA EN TECNOLOGÍAS Y SERVICIOS DE TELECOMUNICACIÓN

ÁREA DE TEORÍA DE LA SEÑAL Y COMUNICACIONES

TRABAJO FIN DE GRADO Nº 1601_044

HERRAMIENTA PARA EL CONTROL DE POSICIONAMIENTO DE UN SISTEMA ESFÉRICO DE MEDIDA DE RADIACIÓN Y DISPERSIÓN EN CÁMARA ANECOICA

AUTOR: GUILLERMO BANCES BULNES
TUTORES: ANA ARBOLEYA ARBOLEYA
FERNANDO LAS-HERAS ANDRÉS

FECHA: 9 de julio de 2016

Contents

List of Figures

List of Tables

1. Introduction

The following thesis is focussed on the development of an mobile hybride application which can be run both on Android and iOS devices. The application is specialized in the use in hospitals and pharmacies. The scope of the application contains the registration, tracking as well as the management of pharmaceuticals and drugs, realized by the technology of RFID.

2. Use, Scope and Limitations of RFID Technology

The following chapter will discuss the reasons why to choose the RFID technology. In the beginning, in the 'Motivation' section there will be described some state of the art applications. After that, the section 'Aim and Scope' will introduce the limits of the RFID technology and of its applications which should be considered during the deployment. In the end, there will be outlined the Strengths Weaknesses Opportunities Threats (SWOT) method to analyze the benefits and threats of an RFID application.

2.1.- Motivation

Concerning the organization and management of medical devices or patients in a hospital, there exist many problems. In the following, some solutions to these problems, as described by Ajami and Rajabzadeh [1], will be depicted.

2.1.1.- Decision Making

First of all, when it comes to decision making, e.g. about the correct treatment of a severe illness, many physicians are stumped for an answer or their opinions are divided. To enable a rapid diagnosis and to improve the patient's health status, 'smart healthcare' [2] would help a lot. 'Smart healthcare' includes RFID tags which are equipped with sensors to ensure the effectiveness of a medical treatment. This accelerates the treatment process a lot. Furthermore, patients or hospital beds equipped with RFID tags make it easier to identify and manage the amount of patients as well as the workflow.

2.1.2.- Internal Communication

Secondly, poor communication between nurses and physicians deteriorates medical supply. For instance, if a nurse notices that a patient needs more tranquilizer because

he became very nervous, she has to tell the doctor to dose the patient with the correct amount. But often, a physician is occupying another patient. So, there exists the problem of communication and further the staff shortage in many healthcare institutions. Thus, inadequate patient monitoring emerges. It should be added that sometimes, there is the risk of misidentification of patients. To explain the last point, one should think of this easy example: At the urology department are two elder patients, Paul Schmitt and Jochen Schmitt. They are not brothers or related to each other and suffer from different types of illness. Paul suffers from kidney insufficiency whereas Jochen suffers from prostatic lithiasis. The first one needs a dialysis every day whereas the second one needs a radiosurgery. Because both patients are unable to walk themselves, nurses and clinical staff have to bring them to the particular treatment room. The problem should be easy to understand, both patients have the same surname but need completely different treatments. If the treatments would be commuted, their health status would deteriorate and they might die because of the misidentification.

2.1.3.- Production process

To give another example of the successful deployment of RFID solutions, Tamm and Tribowski [3, p.110 ff.] outline the company 'Gerry Weber'. In the following, some benefits of the RFID application will be explained. Firstly, count and identification processes of goods could be accelerated by using the RFID technology. Secondly, both the electronic article surveillance and RFID minimize costs and time. Thirdly, the delivery quality was improved and mistakes were reduced and sometimes avoided. Fourthly, the logistic was improved by the improved transparency of stock. Fifthly, the existing heterogeneous systems can be controlled more easily. Lastly, there might occur some reading processes without focus which means that the adjacent items are reflected and erroneously detected. This can be avoided by filtering involuntary readings via software filters.

2.1.4.- Investment possibilities

Another important point for hospitals is the budget and their possibilities to investigate in new technologies which makes the enrollment of a new RFID system more challenging. Furthermore, clinical staff and phycisians have to be introduced into the new technologies. Not only the human factor plays a significant role but also the existing systems, such as the Hospital Information System (HIS), Radiology Information System (RIS) or Laboratory Information System (LIS). If a new identifying system or software shal be integrated into a hospital or healthcare institution, it has to be deployed suitably to the existing system architecture. To achieve the last point, Ajami and Rajabzadeh [1] recommend starting with small RFID projects and mention countermeasures to increase the acceptance of such applications by healthcare institutions. To give an example, the regulations to protect patient's privacy should be mature to achieve more institutional support. Besides, there should exist more customized RFID systems which accomplish the individual tasks of their users.

2.1.5.- Medication Administration System

To explain the positive impact of using RFID systems, in the following, a few applications will be described briefly (see also [1]). Firstly, Ajami and Rajabzadeh describe a Medication Administration System which automatically verifies medication and generates the corresponding prescription. There exist multiple intents of developing an Administration System, such as preventing human errors (like for example mislabeling of tissue specimens in gastrointestinal and colorectal surgery endoscopy units). The second most common error which occured were that patients have been labelled incorrectly. To avoid these errors, an initiative of developing an RFID application to specimen bottles was started. The aim of this initiative was to create a paperless pathology requisition system which correctly confirms boths the endoscopy nursing staff as well as the endoscopist for each specimen bottle. After deploying the application, specimen-labeling errors were significantly reduced.

2.1.6.- Wisely Aware RFID Dosage

Another RFID system, called Wisely Aware RFID Dosage (WARD) system should prevent the risk of medication errors triggered by medical staff. It is based on an integrated barcode and RFID tags which should demonstrate effective and safe patient care environment. Not only the correct dosage can be controlled by RFID but also medical staff. The following paragraph will describe the Mobile Intelligent Medical System (MIMS) which includes a mobile nursing care system using RFID technology. There are many implemented functionalities in the MIMS, such as the tracking of patient's vital signs across various locations and in different medical facilities. The vital sign monitoring enables medical staff to watch critical ill patients carefully and permanently and reduces the risk of serious harm resulting from slow provision [1]. Moreover, it offers alarming services in case of emergencies and can always be taken everywhere. Behind the frontend, a rule-based clinical decision supports medical staff and the mobile nursing environment. Last but not least, MIMS has been extended to most medical domains and has been integrated into other HIS.

2.1.7.- RFID applications in hospitals: A case study

In their conference paper, Wang et al. [4] describe a case study of implementing a RFID system in a Taiwan hospital in the year 2003. The project was named Location-based Medical Service (LBMS) and performed at the Taipei Medical University Hospital (TMUH). In the following section, the development strategy, device management as well as the value generation which were important for developing the LBMS will be explained. Referring to a widely spread disease, called Severe Acute Respiratory Syndrome (SARS) in 2003, the authors Wang et al. discuss the effectiveness of applying RFID in hospitals to prevent further infections (e.g. of patients or medical staff). They mention several challenges of implementing RFID systems in hospitals, for instance user or physician resistance, investment problems as well as technical, clinical, organizational and professional resistance. Nevertheless, some hospitals initiated (with subsidies from the Taiwanese government) preliminary RFID projects as early as October 2003 and achieved significant results.

To give a basic introduction into the existing IT infrastructure at the TMUH, the following paragraph will mention the existing systems of the hospital. TMUH has an integrated HIS that complies with several healthcare standards, such as Health Level 7 (HL7), Digital Imaging and Communications in Medicine (DICOM) [4, p.3 ff.]. Furthermore, the system consists of a LIS, RIS and according to Wang et al. most of the patient's medical records are digitalized. When it comes to the development and the reasons for using LBMS, the authors claim to build a system that could detect and track potential SARS cases. Besides, medical knowledge and practice should form the basis and core for developing the system. The RFID technology was considered as a tool to support medical practice. In the end, the system should reflect medical assumptions. Wang et al. describe a basic workflow with four steps of the LBMS: Initially, all data should be stored in a positioning database which is connected to the existing vital information databases (of the HIS). In the second step, the system automatically retrieves patient medical records from the HIS and runs an inference engine (called 'Rulebase'). 'Rulebase' judges whether there was an infectious event or not. If there was a infectious event, the system detects this in a third step. As a consequence (step four) of the detected event, a message is sent immediately to the relevant personnel through an alarm (email and sms). The LBMS can be extended and used in other contexts, like e.g. for precious equipment tracing, in-patient medicine auditing, new-born baby and mother identification or to legitimate drug control. Wang et al. were supported by the Taiwanese government which approved their plan and granted money. Since the LBMS should be released as a hospital-wide system, the development required expertise and knowledge from different domains, including medicine, RFID technology, IT systems development, telecommunications and systems integration. Actually, three parties were involved: TMUH, Lion Information Inc. and an advisory group [4, p.4] which consisted of professors who emerged the technology and made academic contributions (algorithms). Since the hospital decided that the system should have active real-time position-tracking, temperature taking and monitoring abilities for tagged patients, the developing team chose 916,5 MHz UHF active tags (see Chapter 2, RFID tags **??**) to reduce the risk of staff infections.

Reaching an adequate system integration without loss of performance, functionality and security was a big challenge. With the use of a field generator, a small tag wake-up device that communicates directly with the reader, the real-time communication should be realized [4, p.4]. The generator periodically turns on and calls tags for a specific time. There exist three different types of generators: Normal, floor and area generators. Furthermore, Wang et al. bring up the challenge of the entire device management [4, p.5] with the purpose of collecting and transmitting reads that are as complete and clean as possible. Realizing a complete device management was limited by compartments, rooms, walls and doors because of their buildling layouts and materials which interfere with radiowaves. Besides, the balance between accuracy requirements and investment costs has to be maintained. Moreover, unauthorized removal of tags has to be managed carefully, since there might be some patients who try to take off their RFID wristband. In this case, an additional alarm has to be designed. Basically, the design and deployment of RFID devices depend on the environment and the context in which they are used. Not only the device management was challenging but also the data management as Wang et al. mention. The authors describe two general problems of data management in their RFID system. On the one hand, there will occur intermittent and unreliable reads. These can be compensated by developing algorithms to process missing and incomplete reads. On the other hand, there will be generated high-volume data in a very short time. To prohibit this, the data should be filtered by algorithms and only the necessary data should be transmitted. For instance, if a tagged patient exceeded the present degree of 0.5°C, his data would be transmitted. To come to a conclusion, data management is tied to medical knowledge and practices which can substantially reduce the volume of data to be handled. As a result, meaningful information for decision making will be generated.

Besides the LBMS project [4, p.2 ff.], Wang et al. depict some existing RFID applications. To give an example of a successful use of RFID, the U.S. Department of Defence has been using the technology for years. To give an overview of the usual hospital applications until 2006, Wang et al. describe applications for tracking and managing equipment such as wheelchairs or portable heart monitors. Moreover, trials on tagging patients, staff and equipment in rooms were conducted in several hospitals.

Besides, the Washington Hospital Center (Washington D.C.) deployed a RFID system to track the status and the exact location of patients, staff as well as the essential equipment. During the realization of the mentioned projects, the solutions depended on building an RFID infrastructure together with the middleware and the impedance-matching of the RFID system and the current systems (e.g. Enterprise Resource Planning (ERP) systems). Actually, to get along with the mentioned solutions, a strong team work (involving people from IT and business departments) and project management should be included. Since RFID allows wireless storage and automatic retrieval of data, there exists an 'ecosystem' of companies trying to develop a platform to support RFID development and applications. Besides, the variety of existing systems in hospitals, Wang et al. mention three mayor technical challenges accomplishing a RFID system. First, the non-line-of-sight reading might be a challenge since there exist various types of tags and the frequencies influence the range of signal. Second, handling the serial numbers can be difficult but it could be coped with setting a primary key to each tag which synchronizes with an existing database (see Chapter 3, 'Used platforms and technologies' 49). The third challenge is to deal with the real-time data and to synchronize these seasonably. To deal with that, the use of NoSQL databases makes sense and will be discussed in Chapter 3 49.

Finally, Wang et al. evaluate RFID as an infrastructure technology which allows companies to capture data about objects and individuals moving in the real world [4, p.7]. In addition to that, the authors recommend that organizations should think carefully how to change business processes to reap the benefits of RFID. By naming benefits of RFID, Wang et al. refer to the improved efficiency, patient safety and reduced medical errors which can be very extensive and expensive nowadays [4].

2.2.- Aim and Scope

Ajami and Rajabzadeh [1] mention three important purposes of RFID technology. The first purpose of using RFID is to improve the tracking of objects. It is mainly used to follow products through a specific supply chain or to follow medical devices an drugs in the clinical workflow. There is also the possibility to track a product to a particular

patient or to identify clinicians who administered medication to patients. The second purpose for which RFID technology is appropriate is the inventory management (see section 44). Inventory Management is significant for managing items of an organization, like a hospital. There are many complex processes where information about the location, time and the amount of material is necessary (e.g. towels, duvet covers). The third and last purpose of RFID technology, mentioned by Ajami and Rajabzadeh [1], is validation. Using RFID to identify and validate data is an effective method for ensuring the quality of a hospital or healthcare setting. It ensures that the patient being treated is the right patient.

2.2.1.- RFID and the IoT

There exist many applications, which should help us living smarter, not caring about the ordinary things, like for example turning off the washing machine or closing the windows before stepping out. These smart houses form a part of the term Internet of Things (IoT). Often, the smart solutions are based on RFID technology to identify the exact window or the item that has to be controlled from outside. In their book 'RFID Technologies for the Internet of Things', Chen et al. [5, p.2 f.] depict smart applications and a specific difficulty which they call the 'Tag Search Problem'. It usually appears on large-scale RFID systems and describes the complexity of identifying the wanted tags which exist in the current system. To solve this identification problem, Chen et al. describe the method 'Filtering vectors' which will be explained in the following. Firstly, a compact one-dimension bit array is constructed from the tag IDs which are used for filtering the unwanted tags. After that, a novel iterative tag search protocol is run. This protocol progressively improves the accuracy of search results and reduces the time by using information which were detected from previous iterations. As a second problem of IoT applications, Chen et al. mention the conflict with people's privacy [5, p.3 f.]. Since every tag transmits its ID to the nearest reader, the transmission can be exploited by attackers. To prevent eavesdropping, the authors describe an anonymous RFID authentication mechanism which designs anonymous authentication protocols. The protocol is based on cryptographic hash functions which require considerable hardware to randomize the authentication data in order to make the tags untrackable.

At this point, one should keep in mind that the provided solution requires valuable hardware and is not suited for low-cost tags which augments the production costs. Thus, manufacturers have to face the challenge of designing anonymous authentication protocols for low-cost tags given their limited hardware resources. To face the problem of limited hardware resources, Chen et al. suggest an 'asymmetric design principle' [5, p.4] which means pushing most of the system's complexity to the reader and leaving the tags as simple as possible. Besides the anonymous RFID authentication, tags can be identified by their network [5, p.4 f.]. To give an example, in large warehouses there exists a great number of readers and antennas which must be deployed to provide full coverage. To accomplish the full coverage, networked tags which relay transmissions towards the otherwise-inaccessible reader can be used. As a characteristic of networked RFID tags, they are powered by batteries and rechargeable energy sources (harvest solar, piezoelectric, thermal energy from surrounding environment). Generally, there can be distinguished two types of ID collection protocols: On the one hand, there is the contention-based ID collection protocol which creates too much overhead in multihop networked tag systems. This leads to an increased collision in the network towards the reader and causes excessive energy costs. On the other hand, Chen et al. mention a serialized ID collection protocol. This solution is based on serial numbers that balance the load and reduce worst-case energy costs. As a conclusion, one can say, that imbalanced load in a network leads to worst-case energy costs which should be avoided.

2.2.1.1.- Compact Approximator based Tag Searching protocol

To avoid the above mentioned energy costs, resulting from inefficient protocols, Chen et al. describe several tag searching protocols [5, p.13 ff.] which will be discussed in the following. To begin with, one should keep in mind the method 'Filtering vectors' mentioned at the very beginning of this paragraph in which the tag ID was converted into a one-dimension bit array. This first step can be compared with the first step of Compact Approximator based Tag Searching protocol (CATS), a two-phased protocol to address the tag identification and its polling problem. The idea of CATS is to encode

the tag IDs into a 'Bloom' filter [1] [5, p.15] and to transmit the Bloom filter instead of the ID. Consequently, in the first phase of CATS, the RFID reader encodes all IDs of the wanted tags into a Bloom filter. After encoding, the reader broadcasts the filter together with some parameters to the tags in the coverage area. Each tag receives its Bloom filter and tests whether it belongs to set X. Unwanted tags will be kept silently for the remaining time. Furthermore, a second set Y defines the coverage area of the RFID system. After filtration, the number of candidate tags in Y is reduced. The second phase of CATS deals with the remaining candidate tags from phase 1. These tags report their particular Bloom filter during several time slots. Each candidate tag transmits in k slots and is mapped to a certain set. During the transmission, the reader is listening to the channel and builds a second Bloom filter based on the status of time slots: '1' stands for a busy slot which means that at least one tag is transmitting whereas '0' stands for an idle slot during which no tag is transmitting. These two phases build the main activities of the CATS protocol and seem to be realized very easily. Nevertheless, Chen et al. introduce some raising problems by using CATS. One problem is optimizing the Bloom filter sizes since CATS approximates two Bloom filters together as the first, so that $|X \cap Y| = |X|$. A second problem is that CATS assumes that the first Bloom filter is always smaller than the second one: $|X| < |Y|$. But in reality, the number of wanted tags may be far greater than the number in the coverage area of the RFID system.

2.2.1.2.- Iterative Tag Search Protocol

To avoid the errors caused by using CATS, Chen et al. describe another effective tag search protocol which is called Iterative Tag Search Protocol (ITSP) [5, p.22-28]. Assuming that there is a wireless channel available between the RFID reader and the tag, ITSP interferes from nearby equipment (e.g. motors, conveyers, robots, WLANs, cordless phones). Furthermore, ITSP divides the bidirectional filtration of the tag

[1] A Bloom filter is a compact data structure that encodes membership for a set of items $S = \{e_1, e_2, e_3, ..., e_n\}$. To represent S, a bit array of length l is needed. At the beginning, all bits are initialized to zeros. To encode each element $e \in S$, k hash functions are used to map the element randomly to k bits in a bit array, so that the zeros turn into ones.

search process into multiple rounds. Before each round i, a set of candidate tags in X is denoted as $X_i(\subseteq X)$ which represents the search result after $(i-1)$ round. Thus, the final search result is a set of remaining candidate tags in X after all rounds are completed. So, ITSP can be seen as a general iterative approach allowing multiple filtering vectors to be sent consecutively. Each round contains two phases. During the first phase, the RFID reader constructs m_i filtering vectors for X_i using m_i hash functions [5, p.22]. In a second step, the reader broadcasts the filtering vectors one by one and each tag receives its own filtering vector. By checkiing its ID with the filtering vector, each tag uses the same hash function as the reader. As a result, each tag can get a '1' which means that is it a candidate tag of Y_{i+1} or it receives a '0' which excludes the tag and drops it out of the search process.

Afterwards, during the second round, the reader broadcasts the frame size $L_{Y_{i+1}}$ to the tags (which are all candidate tags) and each tag does the same as in round one. After receiving its filtering vector, each tag randomly maps its ID to a slot in the time frame using a hash function and transmits a response to the reader $(0 or 1)$. After receiving the response from each tag, the reader constructs a new filtering vector which is used to filter the non-candidate tags from X_i.

After the two phases the reader updates the current stage which contains a set of remaining candidate tags. The number of tags shrinks from X_i to X_{i+1} during this step.

2.2.1.3.- Lightweight Anonymous RFID Authentication

There exist many different authentication mechanisms in RFID applications. To give an example of one current possibility to authenticate RFID tags, Chen et al. depict the 'Lightweight Anonymous RFID Authentication' [5, p.39 ff.]. To start with, a fundamental system model is given (see figure 2.1). In addition to the system model, it should be noticed that each tag is pre-installed with some keys for authentication. Furthermore, all readers are deployed at chosen locations and connected to backend servers which are connected to a central server. On the central server, each tag's key is stored.

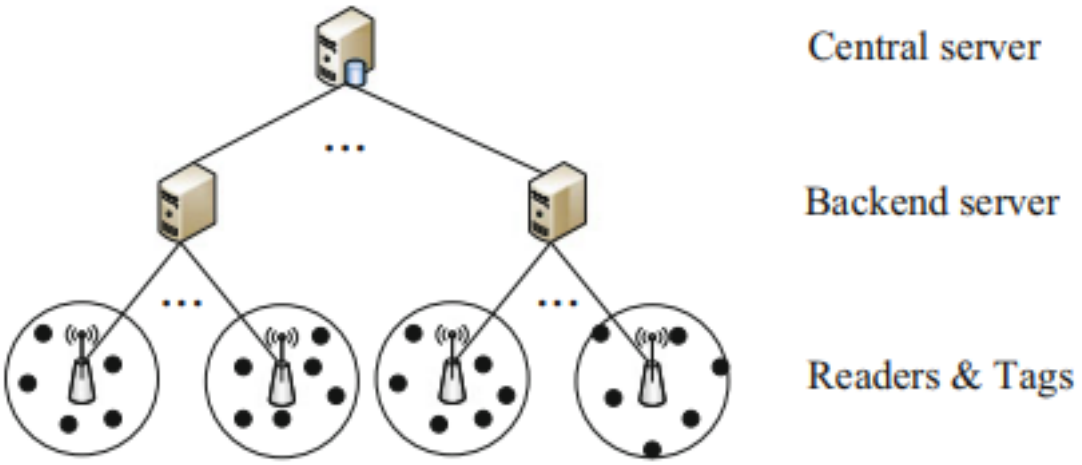


Figure 2.1.- The system model of Lightweight Anonymous RFID Authentication [5, p.40]

Concerning the communication between readers and tags, Chen et al. describe a 'Request-Response mode Communication' [5, p.40 ff.]. Firstly, the reader initiates the communication with the tag by sending a request to it. Secondly, after receiving the request, the tag makes an appropriate transmission as response. There can be distinguished two types of transmissions: Invariant and variant transmissions. The first type (invariant transmissions) can contain content that is 'invariant' between the tag and the reader. In contrast to that, variant transmissions can contain content that may vary for different tags or the same tag at different times, e.g. the exchanged data for anonymous authentication.

2.2.1.4.- Identifying state-free networked tags

Before explaining the mechanism of identifying state-free networked tags, the two terms 'state-free' and 'stateful' networked tags should be made clear. If a networked tag is called stateful, it maintains its networks state which includes information about its neighbors in the network, routing tables as well as update information. In contrast to that, state-free tags serve the purpose of energy conservation and do not maintain any network state prior to their operations which differs them from traditional networks. Given the two definitions, there comes up the challenge of identifying state-free networked tags. Chen et al. refer to that challenge and explain a method for identifying

networked tags [5, p.67 ff.] which will be discussed in the following. First of all, all tags in a network are connected to each other through a peer communication (to the nearby tags). Especially the emerging number of networked tags represents a significant enhancement to today's RFID technology. The problem of readers which cannot cover all tags due to cost or physical limitations can be solved by using networked tags. Moreover, the possibility of peer communication enables a multihop network to be formed among the tags. The transmission range of inter-tag communications is usually short and amounts to about 1-10 m whereas the transmission range of a reader is much larger. Nevertheless, the peer communication realizes a direct two-way communication between the current node and the neighboring node. Concerning the energy input, the energy can be powered through the reader's radio waves but the internal energy should be carried sufficiently for long-term operations (must be made energy-efficient). After establishing a peer-to-peer communication, the reader collects the IDs from all networked tags that are in its read range. Using multiple hops and intermediate tags relaying the IDs of those tags which are not in the immediate coverage area of the reader, state-free tags can be identified.

2.2.2.- RFID and Mobile Computing

Concerning the development of mobile applications in context of the RFID technology, the following paragraph discusses fundamental definitions of mobile computing as well as general architecture patterns, like e.g. Service-oriented architecture (SOA). To start with, Hanhart declares in his book [6, p.9 ff.] the term 'mobile computing' as following: '[...] all processes, activities, applications in a company which are proceed by mobile technologies. The company's staff gets access to data and applications (independently from location and time). The focus is set on man-machine-communication [...]' [6, p.9 ff.]. When it comes to mobile applications which are connected to RFID systems, Hanhart mentions the term of 'Smart things' or 'Embedded systems' which include physical objects, extended by the RFID sensor technology and which are networked to each other. To achieve some understanding among all readers, Hanhart depicts three types of wireless communications technology [6, p.12-13]. Firstly, there exist mobile communications which consist of a service provider and several mobile devices. The

service provider transmits the speech and data from and to mobile devices through a wireless network. Secondly, Hanhart notices wireless local area network (WLAN) which enables accessing to a company's network. To give an example, there exist many WLAN hotspots in hotels and airports, which can be accessed simply. Thirdly, there exist 'wireless personal networks' which connect terminal devices with peripheral devices within small ranges. For instance, Bluetooth or Infrared Data Association (IrDA) are used to transfer data over small distances. Not only Bluetooth and infrared light are used to transfer data, but also ZigBees and Near Field Communication (NFC) is used in many cases [6, p.12-13]. Hanhart describes NFC as a newer technology which consists of an active and passive unit. Actually, NFC is only used for connections of a few centimeters, e.g. in consumer electronics. The active unit can be kept in the mobile because it is very small and the data rate amounts to at least 424 kbit/s.

2.2.2.1.- Basis functions of mobile computing and RFID

When it comes to the use of mobile applications and RFID, one can distinguish between five general scenarios [6, p.13 ff.]. First of all, since RFID enables wireless connection and detection of several items in our environment, it can be used to access mobile applications through the RFID signal. For example, staff can use mobile devices to access (via RFID) business applications and to implement transactions. Secondly, as already mentioned in further sections above, RFID has the main purpose of identifying objects. In combination with mobile devices, there can be established applications which can both identify users and objects. As a third scenario, mobile RFID applications the capture of statal and environmental data. By using sensors, the continuous capture of data is possible. Moreover, smart objects and mobile devices can transform the information directly into actions or convey the data to a central system (or database). As a fourth scenario for using RFID in the context of mobile computing, Hanhart [6, p.13 ff.] remarks the possibility to locate precisely objects and users. Besides, the detected positions can be used to display contextual information or to direct to procedures in backend systems. Last but not least, the purpose of sending notifications in time, can improve and prevent several emergency situations (e.g. in a

hospital). Since objects can send notifications e.g. when reaching a certain state, users get information everytime and everywhere.

2.2.2.2.- Constraints of mobile applications and RFID

Developing mobile applications with the RFID technology not only brings advantages, but also challenges when facing for example the user's needs and requirements. Hanhart indicates some 'constraints' of mobile applications and RFID [6, p.16 ff.] which will be depicted in the following. Firstly, the user interface should be considered. In case of healthcare applications which can be used by nurses, staff and physicians there should exist various user roles and rights. Thus, each user needs his specific interface and only a few (or one single) users are able to see all information of a patient. As a further matter, the mobile application should meet the requirements of connecting quality and service quality. This indicates the exact adaption of a service, specified in the requirements specification document. By the same, the challenge of computing capacity in the developer team should be attended. Furthermore, both principal and agent should be aware of the needed development time to realize all required features (which depends on the size and skill level of the developers). In addition, the technical resources, like e.g. memory capacity and energy supply represent another challenging factor. To deal with the last mentioned challenges, it should be favourable to have some sponsors which can support the project.

2.2.2.3.- Service-oriented architectures

To cope with the constraints and challenges during the development of a mobile RFID application, Hanhart describes SOA [6, p.31 ff.]. SOA is a multilayered, distributed information system architecture which encapsulates parts of an application into business-like services, considering design principles to enable a simplified process integration [6, p.32]. A service can be seen as an abstract software element or interface which provides standardized access to application functions of other applications through a network [6, p.32]. There exist four general design principles with respect to the development of SOA applications. The first design principle

is called 'Orientation of Interfaces' which means that the service interfaces abstract implementation from the user's view. What is more, each service has a stable interface which is technically and functionally defined by its metadata. The second design principle of SOA is 'Interoperability' which can be assured by implementing technical and functional standards. This enables the interoperability of a services and its usage in different contexts. The third design principle is called 'Autonomy and Modularity' which signifies that SOA restructures the applications architecture into autonomous subsystems (domains and services). The aim is to increase cohesion in one system and to minimize the linkage between its subsystems. The fourth design principle of SOA is 'Orientation of needs'. This implies that all services should be oriented towards business objects and process activities in order to provide an approximately granular, functional definable output.

2.2.2.3.1 Domain Architecture The Domain Architecture is a conceptional foundation of SOA. It reveals duplicates in an existing application architecture. Moreover, it is a fundamental decision foundation for service characteristics. Last but not least, it gives a list of possible service candidates which support systematic integration, development and usage of services.

2.2.2.4.- Service-oriented proposal of architecture

In the previous section, the general characteristics of SOA have been discussed. But in which context SOA applications are regularily used? And how is SOA realized? To give answers to these questions, in the following the purpose and integration procedure of SOA applications will be explained. First of all, the conditions and prerequisites for an economic realization of diverse solutions based on mobile computing and RFID are simple and flexible integration into existing system architectures [6, p.133 ff.]. The classical integration of mobile terminal devices involves different middleware components and functions which can have different varieties of architecture (with advantages and disadvantages). Modern application systems are multilayered, for example 3-tier/n-tier-architectures. The three tiers include the client (implemented software-components), middleware (necessary components to connect

client and backend) and backend (business data and functions) tier. The term 'mobile middleware' refers to the extension of the classical client-server architecture with the aim of improved scalability and administration. Not only a mobile middleware is needed for an appropriate integration into SOA, but also a RFID middleware is needed. The following paragraph will mention some functional requirements to this specific middleware. First of all, transformation functions are needed to convert RFID raw data into useful business process data. This includes filtering of errors as well as harmonizing the data formats of different device manufacturers. Secondly, there are configuration functions needed for monitoring and controlling the RFID infrastructure. As follows, a configuration function is able to identify readers, manage configuration data, monitor device functionality and ensure security.

2.2.2.4.1 Classic Integration Mechanism As a third type of integration, concerning mobile computing and RFID, the integration of embedded devices should be considered. Basically, there are three different tiers: Field tier, Automation tier and Management tier. The first tier, Field tier includes the physical connection of sensors, actuators and control units. The second tier, Automation tier, consists of control units which undertake automatic monitoring and processing functions, like for instance the control of temperature. The communication units connect the control units, programming units and the management tier. The third tier, called Management tier, subsists of monitor and control systems and visualizes them to the operator. Additionally, the Management tier delivers software responsive over proprietary interfaces and can be seen as data handling unit. To conclude, the Automation tier can be seen as the communication unit and middleware between Field tier and Management tier. Further, Automation and Management tier can connect to third-party-applications via data interface units.

2.2.2.4.2 Modern Integration Mechanism The last paragraph dealed with integration mechanisms on the real old way. Recently, there are newer technologies and possibilities to realize an integration, such as web services and the emerging communication protocol Simple Object Access Protocol (SOAP). In context of web

technologies and services, there comes up the term Enterprise Service Bus (ESB) [6, p.141 ff.] which provides a standardized interface and communication layer. An ESB is a consistent integration architecture which defines standards as well as central services and provides them for software development, publication and usage. Regarding the integration of mobile applications, the ESB [6, p.143], there are differentiated two types of integration scenarios: a) the mobile client calls directly the provided services from application domains or b) the client keeps communicating with the services via its mobile middleware. If the client wants to call a service directly, he has to implement its Application's Programming Interface (API). Besides, for service call or invocation, the standardized interface technology has to be used. In the matter of integration of RFID systems and embedded devices, the middleware of RFID systems uses the provided services of the application domains, provided by the ESB. In addition to that, mobile applications can be integrated both online and offline [6, p.146 ff.]. Hanhart is using the term 'online' in context of saying that the mobile device runs the user interface. This indicates that the mobile middleware prepares contents of application (for prompt). After that, the application accesses the backend or invoked app through a service which uses the application's functionality via services. In contrast to that, Hanhart uses the expression 'offline' in order to say that the application is running on the client. Here, the mobile application acts as an invoked application and synchronizes its data through the mobile middleware with the backend. The central management of process states (on the client) and synchronization with services are realized through the middleware directly.

2.2.2.4.3 Capabilities of SOA, mobile applications and RFID To explain the capabilities of the above discussed technologies and architecture, Hanhart brings up 'Reuse', 'Isolation of Domains' and 'Easy implementation'. Reuse is generated by consistent functionalities of interfaces. Isolation of domains is produced by separation of concerns and core data concepts. Easy implementation refers to cross-domain workflows or taskflows. Concerning possible usage scenarios, Hanhart mentions some examples [6, p.207 ff.], like event-driven process management which includes the automatic capture of events. Or, if it comes to the control of several processes and

activities in a company, these activities can be executed by using mobile phones or tablets. Additionally, they will record the encountered states. Concerning the 'ecosystem' and exchanges in it, Hanhart talks about some upcoming challenges [6, p.212 ff.], like the realization of mobile solutions. It is important to consider the high costs of hardware and software. In addition to that, the complexity of integration of solutions and backend systems has to be assumed very well. Lastly, there should be staff who configures and operates the mobile devices.

2.2.2.4.4 Examples of SOA applications Hanhart mentions several use cases of mobile applications and RFID. In order to depict two of his examples, the following paragraph will explain firstly the case study: 'Fraport AG' [6, p.39 ff.] and secondly a Workflow-Management System (WfMS) [6, p.204 ff.]. To start with, Fraport AG is a company which is simulataneously owner and operator of Frankfurt airport. By including the RFID technology and mobile devices, several solutions have been realized in processes for mobile support of staff and in use of real-time data. The scope contained the maintainance of fire dampers and mobile support of loadmasters during loading respectively unloading and mobile capture of booking of goods input and goods issue in stock. The second example Hanhart notices, is a WfMS [6, p.204 ff.] which is able to control processes, e.g. in companies. To realize a WfMS, the workflow client needs to be installed on the mobile device. Following, RFID systems and embedded devices are able to report events to WfMS and can trigger or control processes on the workflow integration layer.

To give an outlook of the possible extensions of mobile applications and RFID, Hanhart explains some fundamental concepts [6, p.208 ff.]. The first concept is called 'Emotion-Silent Process' and is based on sensors, actuators, artificial intelligence which includes the learning from given data and derive several activities. In the given usage scenario (which refers to a hospital or retirement home), sensors firstly detect the movement of a elder person. After the detection step, the sensor's information are connected to further data (e.g. time) with the help of pattern detection algorithms. Finally, the aim of the 'Emotion-Silent Process' is to detect and prevent emergency situations by sending an alarm to responsible persons (like physicians or nurses).

Furthermore, the process is called 'Emotion-Silent Process' because of the 'silent' protection of people which should obtain the independance of these people. A second usage scenario which is noticed, is called 'Velocity-Outtasking and Application Outsourcing'. Based on the spread of web services in cross-company cooperations either external access to single tasks and functions ('outsourcing') or to whole applications ('application outsourcing') can be accelerated. The term 'Outtalking' is used to talk about web services of external providers which can be incorporated to the own service repository and are centrally available for further usage. In contrast to that, 'Application Outsourcing' refers to externally obtained applications (from application-service-provider (ASP)) which can be integrated through the company-internal ESB into the system landscape.

2.3.- Analysis of RFID applications and their use

Often, there not only exists one ideal solution for implementing RFID applications, but multiple applications. In order to decide whether the proposed solution is the appropriate one, the SWOT method has been established [3, p.47 ff.]. SWOT is the acronym for strengths-weaknesses-opportunities-threats and can be seen as the epitome of a popular instrument for self-analysis of decision makers. The analysis itself can be divided into two comprising steps: In order to achieve the objective with the given system, its strengths and weaknesses (with an internal origin) are identified in the first step. After that, the system's environment is analyzed by ascertaining external opportunities and threats. To give an example of the SWOT analysis, Tamm and Tribowski [3, p.47 ff.] consider two perspectives on RFID applications: The 'Enterprise Perspective' as well as the 'Political Perspective' which will be described in the following. From the enterprise's point of view, the strengths of RFID systems are the optimization of operational processes and the reduction of costs. Further, many enterprises improve their transparency because of the raised quality of data (improved decision making). In contrast to that, there exist weaknesses of RFID applications from the view of enterprises, e.g. the challenge of integrating them into the IT, the physical as well as the organizational integration of processes. When it comes to the environmental analysis of enterprises, there occur some opportunities, like for

example new business models which are based on RFID. Or, for instance there will arise innovative business partners which cause a general willingness to cooperate with them. On the opposite, there also might occur some threats in the context of RFID applications in enterprises. To give an example, there might appear an asymmetrical cost-benefit in the value chain. Moreover, any application standards are missing to establish a cross-company infrastructure [3, p.47 ff.]. From the political perspective, the strengths of RFID applications are receptive RFID users, effective manufacturers of the technology, exploratory infrastructure and strategic projects. In contrast to that, the weaknesses of the mentioned systems could be the risk of investment at Small and Medium-sized enterprises (SME), an inadequate alignment of the technology in Europe and missing application standards. As external opportunities can be seen the high potential to gains in efficiency, the emerging new employments, the market share for european technology manufacturers and the resulting data privacy technologies. On the other hand, Tamm and Tribowski [3, p.47 ff.] mention political threats which might exist in the german point of view. For instance, there might occur competitions in technology development with the USA and Asia, rising discounters beyond Europe, missing global interoperability as well as a missing consensus of sociopolitical problems.

According to Tamm and Tribowski [3, p.95 ff.], the highest potential of the RFID applications is the cross-company deployment of RFID because of the raised visibility in a cross-company solution. Generally, the benefit of network technologies depends on the deployment of the application in the network as well as on the number of partners which are integrated into the application. Nevertheless, cross-company RFID solutions enable cost reduce due to the distribution of costs to multiple stakeholders and because of the multipurpose of their transponder.

2.3.1.- Process Model

When establishing a RFID system in a company or building a cross-company infrastructure, in practice, process models are used to roll out. Process models divide a process into definite phases [3, p.59 ff.] which can be named as the following: 1) prephase, 2) analysis phase, 3) draft phase, 4) implementation phase and 5) adoption

phase. In the succeeding paragraph, each phase will be depicted briefly. Firstly, the prephase includes the definition of determine aims, the project team, requirements to the application, funding models and approach. After that, in the second phase (analysis phase) information about all stakeholders is collected. Afterwards, all used IT systems are analyzed in order to integrate the RFID technology correctly into existing applications. Besides, the technical infrastructure is analyzed to find out the technical characteristics of RFID. In addition to that, the functional requirements are defined. In the third phase, the draft phase, the target process is the documentation of the functional specification document which is based on the specification book. Next, during the implementation phase, the software is developed and tested, hardware installation, configuration, tests are performed. Every action as well as every result is documented and later used as training material. All in all, this phase aims to implement an operational solution which can be adopted to the existing systems. Before the last phase, qualification measures for all stakeholders are performed in order to check the appropriateness of the application to the specified requirements of phase three. In the last phase, the adoption phase, the developed application is adopted and released. With the adoption, the maintainance phase of the application starts. To conclude this recommended process model, one should consider that it is only a 'model' described by Tamm and Tribowski [3, p.59 ff.]and project-specific variables like e.g. number of team members or ressources can influence each of the stated phases.

3. Functionality of RFID technology

3.1.- General Information

According to Ajami and Rajabzadeh [1] RFID technology is capable of an automatic unambiguous identifiation without being placed in the line of sight of their objects. The data between RFID tags and readers is transmitted through radio waves. In the 1940ies, the technology was firstly used to identify airplanes during war. Today, it is used in several different areas, like for example in manufacturing, supply chains, agriculture, transportation systems, healthcare services etc.

3.1.1.- Components of an RFID application

Ajami and Rajabzadeh [1] mention five main components existing in a RFID system. Firstly, there is the RFID tag attached to an object ensuring its unique identification. Secondly, the RFID reader detects each tag and creates a magnetic field. In order to detect tags, one or more antennas have to be connected to a reader. Thirdly, in every RFID system has to exist a communication infrastructure which enables the interaction of readers and tags through an Information Technology (IT) infrastructure. Lastly, to enable users to connect to the RFID infrastructure and to control its modules, there has to be established an application software including an user interface and a backend service (e.g. database).

3.1.1.1.- RFID tags

Henrici [2] states that there are two types of RFID tags: Tags with 'Smartcard'-like functionality and 'Auto-id' systems. The first type of RFID tag provides extended functionalities and has computational capabilities. Furthermore, sensors can be attached to the 'Smartcard'-like tags which measure and control temperature and can

be used for telemetry applications. Basically, RFID systems can be seen as a subset of 'Auto-id' systems.

According to Tamm and Tribowski [3, p.15 ff.] who refer to the 'EPCglobal' (an industrial consortium) which proposed a separation of RFID transponders (tags), there can be distinguished five classes . The first three classes include passive tags which have no own energy or power supply whereas the last two classes are used to identify active tags. Particularly, the 'Class 0' signifies that the serial number is written during production process. The 'Class 1' means that a transponder can only be labelled once. 'Class 2' means the tag is rewritable, e.g. the serial number or further data can be rewritten. 'Class 3' represents the tags which have their own internal battery for a microship but whose data exchange (sending and receiving information and messages) is supported by the reader's energy. When it comes to the last two classes, Tamm and Tribowski remark the purpose of reassessment, aggregation and transformation of RFID data. Actually, these active tags are no 'real' RFID transponders but 'telemetry transmitter' because they do not influence the electromagnetic field of the reader and do have their own electromagnetic field. In particular, 'Class 4' refers to tags which have their own power supply which is used for the microship and data exchange. Furthermore, they cannot communicate with passive transponders. The final 'Class 5' appoints to tags which can also communicate with passive transponders.

When it comes to the variety of RFID tags, three fundamental types are distinguished: Active, semi-active and passive RFID tags [2] which all consist of an antenna, a microchip and packaging. Active RFID tags consist of a microchip and have their own power source. As a characteristic, they are more expensive than the other two types. After that, semi-active tags or also called 'hybride' tags have their own power supply which is only used to support the microchip. The transmission or communication between semi-active tag and reader is implemented by using the power of the reader's field. Lastly, the passive RFID tags do not consist of a power source and only work in the reading range of the reader. They harvest their needed energy from the electromagnetic field of the reader and are cheaper than active tags. Moreover, passive tags are lighter than active tags and provide a long-lasting service. In constrast to active tags, passive tags are limited in their read range and functionality.

According to Henrici [2], the memory capacity of passive RFID tags can vary from single bits to kilobytes which is not much. As a recommendation, an external database to store tag-specific data should be used. For instance, a memory of 12 byte is very common to store Electronic Product Code (EPC). Concerning the memory technology, Henrici distinguishes two general types of storage: non-volatile and volatile storage. Non-volatile storage can be divided into read-only (fixed after manufacturing), Write Once Read Many (WORM) and read-write which set the access privileges to the memory. The opposite of non-volatile storage is called volatile storage and is used for example to perform calculations after power-up. Besides, Henrici mentions tags which are able to check passwords or implement ciphering algorithms to ensure data privacy. To visualize the tag's data and to provide real-time measurement, passive tags can be equipped with displays, buttons and temperature sensors.

To maintain the security and authenticity of each RFID tag, Henrici [2, p.93 ff.] depicts four implementation methods of identification. The first and easiest method is called 'regular identification'. It implies that each tag sends its complete identifier to the reader within a Single Logical Message Exchange (SMLE). Another method is called 'implicit identification'. It uses information that has not been provided explicitly for particular identification purpose. Thirdly, a more sophisticated and secure method to identify tags which is the 'multistep identification' method. As the name of this method is very self-explaining, one should image the next three identification steps: In the first step, only parts of the identification information is revealed. After that, an authentication and authorization step follows. Once, being authenticated and authorized, more identification information will be revealed. Other than the mentioned methods, Henrici describes a fourth and most secure method to identify tags which he calls 'encryption and shared key identification'. As an advantage, this identification method protects every information contained in an identifier which can be transmitted in encrypted form. The vast amount of information requires a high internal storage of the tag, like given by active tags. To arrange an encrypted transmission of the information from passive, low cost tags the identifier needs to be calculated outside the tag and then stored on the tag (directly in enciphered form). So, there would be no additional expenditure to enable encrypted and shared key identification.

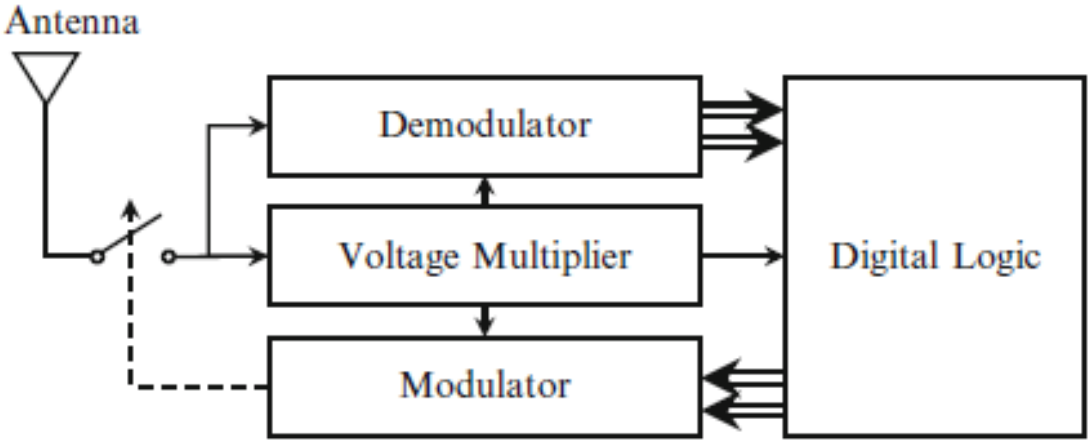


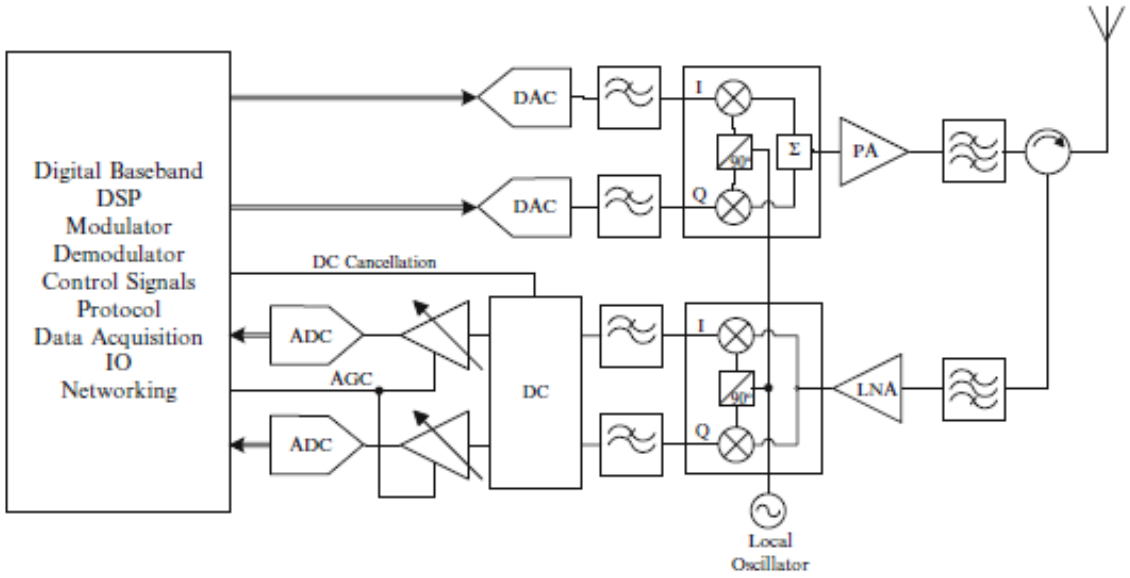
Figure 3.1.- The design of RFID tags [7, p.13]

As above mentioned, RFID tags can be categorized in different ways. In contrast to Tamm and Tribowski 26, Rezaiesarlak et al. [7] describe three different categories [7, p.9 ff.]: Firstly, there can be distinguished between inductive and radiative tags. Inductive tags are the ones which work below a frequency of 100 MHz whereas radiative tags in the Very High Frequency (VHF) range (30-300 MHz) or above. Secondly, there can be differentiated between active and passive tags as mentioned above. Lastly, there are both chipped and chipless tags (see Section Chipless RFID systems 32).

3.1.1.2.- RFID readers

In this section, RFID readers will be explained in detail. To start with, one has to imagine existing objects which are tagged with a RFID tag. To implement functionality to these tags and to connect them to a middleware or a backend system, a detector is needed. This detector is the RFID reader which consists of an antenna, a power supply for passive tags, a microprocessor (to control devices) and an interface for forwarding data to the processing backend system [2]. Generally, two different types of readers can be distinguished: Stationary and mobile readers. Stationary readers need to be integrated into the existing system architecture by additional middleware [6, p.133 ff.]. Likewise, direct coupling between application systems is not possible because of the amount of data which has to be handled, the lacking ability of being a real-time system and the limited possibilities of RFID readers to produce the required process

information. To give an example of the use of stationary readers, they are oftenly used for goods receiving or stock management. Furthermore, stationary readers are fixed to a specific location and need permanent network connection. Additionally, the antenna and reader are spatially separated from each other [3, p.17 ff.]. On the opposite, mobile readers do not need permanent network connection and are used for instance to query prices in a supermarket. They are usually integrated into mobile devices, connected to laptops, Personal Computer (PC)s or tablets. To connect themselves to an existing system, mobile RFID readers need a device driver which enables the communication between reader and the installed application on the device [6, p.133 ff.]. Furthermore, the antenna as well as the reader itself are integrated into their casing [3, p.17 ff.]. Nevertheless, there exists the possibility of conntecting various antennas to one reader to extend the range of field. As mentioned in the section before 25, RFID tags and readers communicate via electromagnetism. The reader's detection range depends on the frequency as well as the electromagnetic field [2]. In general, four frequency ranges can be differenced: Low Frequency (LF) (125-134 kHz),High Frequency (HF)(13,56 MHz), Ultra High Frequency (UHF) (868 MHz-915 MHz) and Microwave (2,54 GHz-5,8 GHz). Each frequency range has its own physical characteristics, such as the needed size of antennas or the read range. According to Vizinex [8], an american company with site in Pennsylvania (U.S), HF tags can be used for short read ranges (up to 3 inches). They are usually tagged to tissue samples, blood and critical fluids. Furthermore, HF tags work well in proximidity to liquids as well as human tissues. UHF tags provide longer read ranges and can be detuned by proximity to tissue, fluids and metals. These tags are typically used to track and locate critical medical devices, manage inventories of medical items and track as well as identify patients. Moreover, UHF tags are compatible with worldwide standards and easily deployed because of the compatibility with widely available and competitively priced RFID readers. Furthermore, each reader has its own electromagnetic field. Such fields are distinguished into near field and far fields: Near fields, also called magnetic or electric fields work with induction and capacitive coupling whereas far fields consist of electromagnetic waves. The measuring unit of electromagnetic fields is called field strength and the maximal field strength depends on national regulations. These national regulations limit the electromagnetic compatibility to avoid disturbing



The design of a RFID reader

Figure 3.2.- The adopted from [7, p.17]

other systems. The functionality of passive tags within near field is different from passive tags in far field. In near field, the tags send data to the reader using load modulation. This mechanism does not work in far fields: Here, the sended frequency is backscattered [2]. All in all, readers are able to query tags and to read and write tag data. But the storage of information and the information processing does not take place in readers or tags, but in the middleware or backend systems. These will be explained in the following paragraph.

3.1.1.3.- RFID backend systems

As Henrici [2] mentions, the backend can be divided into two parts: Middleware and applications. Both of them run on the same computer within the same network which is important for the permanent connection to RFID readers and all existing tags. The advantages of a middleware in this use are that no adaption of appications is needed, an open and neutral interface for other applications is provided. Besides, as the middleware is used to aggregate and filter data, the tags only have to identify objects. As a result, modularity of the system is maintained.

3.1.1.3.1 RFID Middleware The RFID middleware can be defined as follows: '[...] the software component for preparation and deployment of RFID data which enables the integration of RFID readers and further infrastructure into the operational application systems [...]' [3, p.20 ff.]. According to this definition, there have to be considered three fundamental functions of the middleware: Reassessment, Aggregation and Tranformation. To start with, during the reassessment, all received data from the antennas can be redundant or flawed. This redundance is caused by different antennas detecting the same RFID transponder at a time or because one RFID transponder has been detected multiple times during one time frame. Flawed means that transponders were not detected in the intended field or they were detected incorrectly. In second place, aggregation defines the process of summaring all contextual information into one single RFID information ('together into one'). In third place, the term 'transformation' is used by syntactic and semantic means. To come to a conclusion, the RFID middleware improves the management of readers by abstracting from technical details. Furthermore, it provides a scalable solution which reduces the unneeded complexity which is transmitted to the users [3, p.20 ff.].

3.1.1.3.2 Data storage concepts Concerning the data management of RFID systems, Tamm and Tribowski suggest three general concepts of storing tag-specific data: 'Data-on-Tag', hybride forms and 'Data-on-Network' [3, p.22 ff.]. 'Data-on-Tag' is a highly recommended method because of the decentral data storage. It improves the user's privacy accessing object-referred information. Moreover, the 'Data-on-Tag' strategy is useful if only relevant and necessary information are contemporarily needed. In addition to that, if the system is not available, the processes can be executed with the tag's information. Furthermore, 'Data-on-Tag' brings many advantages with it like for instance a raised reliability of the entire system because the processes are decoupled from central system components. On the contrary, 'Data-on-Network' implies a central data storage. Further, it can be easily standardized because only the identification number has to be standardized. Further, the only additional requirement remains the working network connection. Mentioning the different data storage concepts in RFID systems brings up another term which is used to detect e.g. product piracy: Complex

Event Processing (CEP). CEP uses compound read events to detect the multiple capture of one identification number (at different places). If multiple captures of the same identification number are found, the mechanism concludes to a copy of the RFID transponder.

Actually, data is barely stored on RFID tags because of the limited resources in low-cost tags. It is recommended [2] to store tag information on an encapsulated database. As an advantage, databases provide high flexibility to change data or to execute queries without the tags being present. Furthermore, the backend infrastructure should use a Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol to ensure a secure transmission of data. Finally, the data would be transmitted and stored in a backend infrastructure on a central storage [2].

3.1.2.- Functionality of RFID system

When developing an RFID system, it is important to think about the unique identification of each object. To enable a reliable identification of objects, only one RFID tag should be attached to each object. The tag itself has a 'read-only' or in some cases 'rewrite' internal memory which enables users to get or change the object's information [1]. Secondly, the RFID reader generates magnetic fields to enable the RFID system to locate objects (via tags) within its range. Additionally, the high-frequency electromagnetic energy and the query signal which is generated by the reader triggers tags to reply to the query. Each query can have a frequency of 50 times per second [1]. Thus, it is possible to generate large quantities of data which have to be filtered by supply chain industries. Each filter is routed to a backend information system, using a software similar to 'Savant' which is used to control the data. 'Savant' acts like a buffer between the HIS and the RFID reader [1]. Besides, Tamm and Tribowski [3, p.18 ff.] distinguish between three classifications of RFID systems: 'Close-coupling-systems' ($\leq 1m$ range), 'Remote-coupling-systems' ($\leq 1m$ range) and 'Long-range-systems' (¿1m range).

3.1.3.- Chipless RFID systems

3.1.3.1.- Comparison: Chip-based vs. Chipless RFID systems

Besides chip-based RFID systems, there exist chipless RFID systems. In their book, Rezaiesarlak et al. [7] describe the differences between the two RFID systems which will be depicted in the following paragraph. Generally, RFID tags are one of the currently proposed candidates which can compete with traditional barcodes. Furthermore, there exist 'conventional' RFID tags which can handle the communication's protocol by using electronic circuitry in their structure. In the year 2002, especially UHF RFID tags were used and stimulated a large-scale movement in industry and academia. UHF (see Section RFID reader28) allows a longer read-range as well as a faster reading procedure which extends the range of applications. Moreover, there has been established an 'UHF RFID Tag Design' which refers to the essential modules of an UHF RFID application: The antenna, voltage multiplier, digital logic and memory as well as the demodulator [7, p.12 ff.]. Analogous to the 'UHF RFID Tag Design', Rezaiesarlak et al. mention the 'UHF Reader Design' which relates to readers. The reader receives the tag's signal with the same frequency at a time that transmits a 1 W **CV!** (**CV!**) signal to keep the tag ON. The circulator, also called ring coupler, would allow to separate the transmitted signal from the received signal. After this separation, the reader runs with an isolation of 20dB which can be raised if needed by using separated antennas for transmitter and receiver. To establish a connection, the tag itself uses time-variant Radio Communication System (RCS) by impedance modulation of the antenna. On the other hand, chipless RFID tags do not have any electronic circuitry in their structure, which makes them easier to manufacture. In addition to that, chipless tags consists of a fully electromagnetic scatterer and encoder. Using conductive ink, conventional inkjet printer are able to print tag pattern easily and directly on the product package or item. As a disadvantage, Rezaiesarlak et al. [7, p.12 ff.] mention the difficulty of the detection technique using chipless RFID tags. For example, in an environment containing multiple tags, noise or clutter (means interference) it is very challenging to detect the correct tag because of the occuring reflections from the background which are stronger than the tag's response.

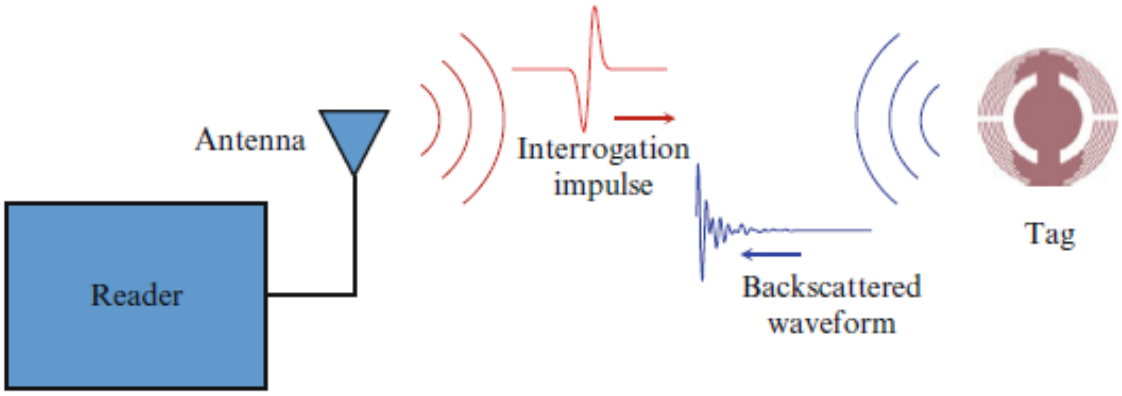


Figure 3.3.- The architecture of chipless RFID systems [7, p.17]

Figure 34 represents a simplified architecture of a chipless RFID system. The main difference between this architecture and the architecture of conventional RFID systems is the communication between reader and tag. These are realized by an 'Interrogation impulse' sent by the reader and a 'Backscattered waveform' reflected by the tag. Experts talk about a Frequency-Modulated Continuous Wave (FMCW) chirped radar while discussing chipless RFID systems.

As already mentioned, chipless RFID tags act both as scatterer and encoder. They employ static information incorporated in complex frequency domains of the tag[7, p.18 ff.]. Concerning their exact structure, the given figure 35 explains some features of chipless tags. To start with, each chipless tag is made of an arbitrary metallic body with some narrow-band-resonant frequencies which means that these are resonant structures like mono poles, dipoles, rings half-wavelength slots or quarter-wavelength slots. As mentioned above, chipless RFID tags can be constructed very easily: By using a planar metallic patch with a few quarter-wavelength slots as identifications.

Not only the chipless RFID tags are important for developing a chipless system, but also the chipless readers have to be considered. As Rezaiesarlak et al. [7, p.18 ff.] explain, chipless RFID readers do not have any integrated logic circuitry to implement any communication protocol. This makes the detection procedure even more challenging compared with conventional UHF tags. Nevertheless, the reader should be able to extract complex natural frequencies from a scattered signal which will collide with signals from other scatterers or tags. As can be seen from figure 36, the proposed

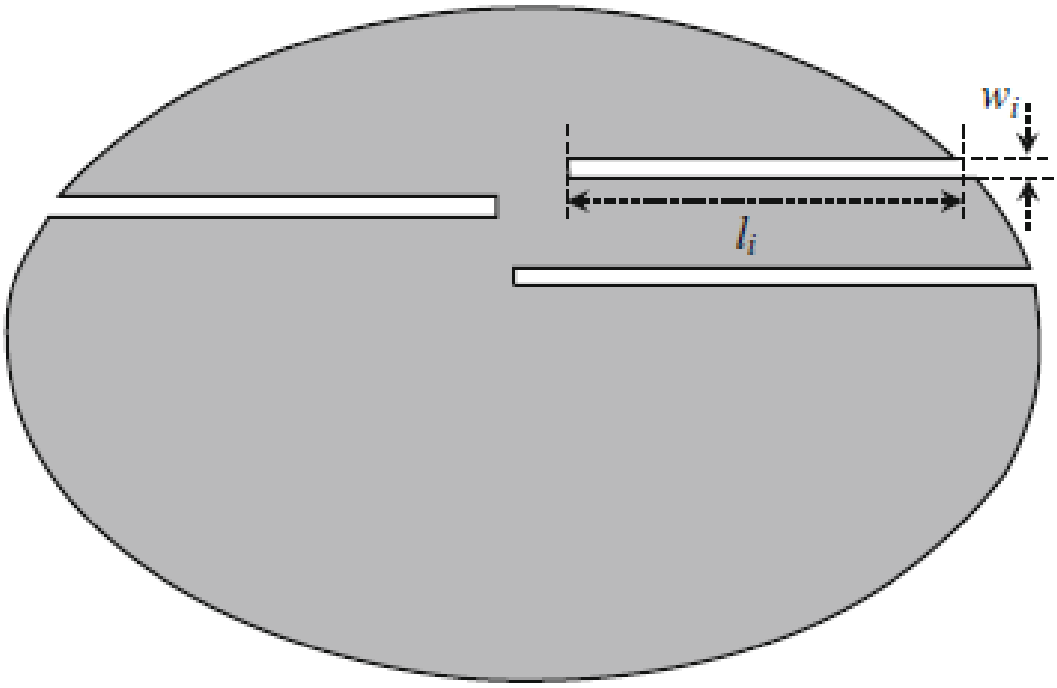


Figure 3.4.- The design of chipless RFID tags [7, p.19]

Ultra Wide-Band (UWB) (3.1-10.6 GHz) reader uses a direct-down-conversion in the receiving path to overcome the transmitter interferences. Both transmitter and receiver can have two different UWB antennas or share one antenna and one UWB circulator.

3.1.3.2.- Design of chipless RFID tags

When it comes to the development and use of chipless RFID tags, one has to keep in mind that these tags are composed of both a scatterer and an encoder. The scatterer reradiates incident fields which means that the signal-to-noise (SNR) signal-to-noise ratio in the reader is being maximized. The purpose of the encoder is to encode the data on a backscattered signal. To design appropriate tags for those readers, there exist two possible designs. The first one is called 'time-domain reflectometry-based (TDR) design'. It implies that each tag includes some discontinuities along a long transmission line. The positions of the discontinuities encode data by a train of pulses. This train is shifted correspondingly to the positions of the discontinuities. To give an example, surface acoustic wave (SAW) tags include a design based on TDR. The second design is called 'spectral-based' design. Here, the tags' ID is incorporated into the spectral

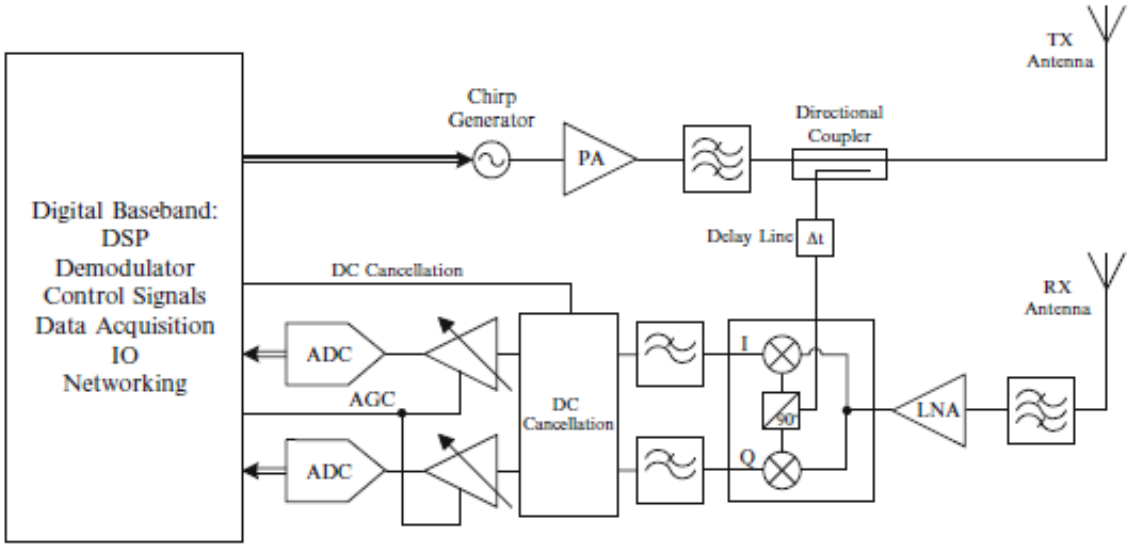


Figure 3.5.- The design of chipless RFID readers [7, p.20]

response of the scattered signal. The frequency band of operation is divided into N sections corresponding to N bits. When talking about the appropriate design of such chipless RFID tags, there will come up the questions about the need for each systematic design. As encoder, the quality factor needs to be considered as well as the resonant frequency tunability of embedded resonators. As scatterer, the residue of poles and radar cross section, dependency on polarization and direction of the tag should be considered. There exist two possible design approaches which are based on the characteristic mode theory (CMT) and singularity expansion method (SEM). The CMT is a resonance-based design of chipless RFID tags which uses the phenomenon of studying the resonant and radiation characteristic of a tag by decomposing the current distribution on the tag into its characteristic modes [7, p.81 ff.]. If there are multiple chipless tags in an area, it is recommended to use SEM which writes the current density of tags as a summation. Furthermore, SEM enables the expansion of the currently found tags to build them into a series of complex natural resonances.

3.1.3.3.- Detection, identification and localization in chipless RFID systems

3.1.3.3.1 Detection To begin with the general functionality of detection of chipless RFID tags, it is important to mention that the scattered signal from the

RFID tag is received by the receiving antenna which transfers it to the reader [7, p.127 ff.]. After that, the reader extracts the same information such as the tag's location and ID from the received signal. In case of applications where multiple tags are presented, the detection process can be divided into two steps [7, p.127 ff.]. In the first step, the reader distinguishes all tags which are in the reader's area between responses of background objects around the tag. Afterwards, the tags' locations and IDs should be extracted from their identification information. To distinguish between multiple tags in one area, there exist further anti-collision algorithms to separate the ID of the tags.

3.1.3.3.2 Identification When it comes to the identification process of chipless tags, it should be depicted that each ID is generated by arranging resonant frequencies of structure [7, p.129]. Moreover, the ID is included in the late-time response of the received signal. Additionally, a time-frequency representation is needed in order to extract the ID of the tags from the late-time part. Besides, cases where multiple tags are in the main beam of an antenna, another dimension for space should be added to the representation diagram. The proposed mechanism is also called 'space-time-frequency representation'. It enables obtaining all the required information of the tags. Nevertheless, the identification process in chipless RFID system can be expanded in many regards, such as to improve the system's performance. In this regard, one should consider the resolution of the applied algorithm in space, time and frequency domains.

3.1.3.3.3 Localization Discussing the localization in chipless RFID systems primarily brings up the desire of an exact and precise location of a tag in the reader's area [7, p.143 ff.]. By knowing the exact location of a tag, the reader antenna can direct the antenna bearn to the object, suppressing the interference signals from background objects. Likewise, enabling the capability in chipless RFID sytems, it can be used in a wider range of crucial applications, such as health-care monitoring in hospitals. Concerning the ranging techniques, Rezaiesarlak et al. [7, p. 143 ff.] propose two ranging methods. The first ranging technique is called 'time-based ranging' and is based on the time of arrival (TOA) of each signal. Whereas the second ranging technique which is called 'signal-strength-based ranging' is based on the principle that the greater

the distance between two nodes is the weaker will be their received signals. If the two ranging techniques are compared, the 'time-based ranging' will bring the advantage of ultra-wideband technology in the detection process and will be more precisely and accurate than the 'signal-based ranging' method. According to Rezaiesarlak et al., most chipless RFID applications use the classical matched filter (MF) whereas the TOA estimator is used to find the time when a signal has its maximum peak. The backscattered response from each tag includes an early-time and late-time response. Dealing with multi-bit tags, the late-time response of each tag is composed of high-Q sinusoidals corresponding to embedded poles on the tag. If some sinusoidals are in-phase, their effect might be constructive enough to strengthen the late-time response at those time instances. If two ore more tags are located in one area, the early-time response of a second tag might be hidden in the late-time response of the first illuminated tag. For bi-static cases, there is no guarantee that the early-time response is stronger than the late-time response.

3.1.4.- Security and Privacy of RFID systems

Security and privacy in the healthcare sector is a very important and highly discussed issue. As these are very large issues, which could not be described within a few paragraphs, there will be depicted some examples of threats. In the second section 'Solutions and Methods against Threats' 41, five important recommended countermeasures will be described. At this point, especially the term of privacy should be defined clearly. According to Tamm and Tribowski [3, p.90 ff.] privacy stands for the right of an individual to keep certain aspects of his life private. Aspects refers to the informational self-determination which should not be controled by further instances, like e.g. systems or third-parties. Additionally, privacy is considered as basic right which is also defined in the Federal Data Protection Act and includes explicitely the protection of personal data.

3.1.4.1.- Security Problems and Threats

As Henrici [2] mentions, there exist two fundamental fears about the RFID technology. The first fear concerns marketing purposes, such as creating very detailed customer profiles which lead to a vast amount of information. Secondly, the technology offers the possibility to keep people under surveillance which implies advantages and disadvantages. As an advantage, the patients' life gets more confortable and companies will be more productive. As a negative result, people's privacy is violated and the application's security is not addressed properly. Aside from the two fears, Henrici describes several risks of RFID systems, such as the ease of disrupting the service which indicates data security and privacy problems. When talking about security, one should distinguish between security of systems and services and the security of data and information. The last point can only be ensured by secure systems [2]. In the following, some security and privacy risks using RFID technologies will be explained. To start with, one should think of his passport and the data which is stored on it. The new passports have an internal RFID tag which enables readers nearby the passport to read out all data and to copy them as well. As mentioned in section 25, passive RFID tags are cheap, do not have their own power supply and can be read through a nearby reader. So, reading out the passport's data would not be very complex. Moreover, Henrici mentions product counterfeiting in pharmaceuticals which can cause a lot of harm, like the death of patient's. Nevertheless, the drug market is bound to strong regulations, like for example through the Federal Drug Administration (FDA). To detect and reduce product counterfeiting, RFID tags need to prove genuineness of original products to patients and should inhibit cloning them.

In his book, Henrici mentions six cases of possible attacks to RFID systems [2, p.61 ff.]. The first attack is called 'Illegitimate reading of data' and describes the possibility of side-channel attacks which use the communication protocol between passive tags and backend systems. As described in section 'RFID backend systems' 30, passive tags are used more often and are less expensive than active tags. Nevertheless, the vulnerability of synchronizing each tag with the backend system through a protocol enables attackers to bypass normal protocols so that they can readout all transmitted data. The second

possible attack, Henrici mentions, is called 'eavesdropping of data'. It is caused by the problem of the public and shared communication channel between readers and tags. Compared to 'illegitimate reading of data', everybody near enough the communication channel is able to eavesdrop the conversation because of the use of passive tags. Particularly the 'forward' channel from reader to tag has a stronger magnetic field than the opposite direction which makes it more easily being eavesdropped than the backed one. Thirdly, Henrici declares 'cloning or mimicking of tags' as a third threat. His definition of cloning a tag is restricted to creating an exact logical copy of an item which is not distinguishable from the original tag on the protocol level. There might exist some minor differences like the power consumption or time response but the replica cannot be detected with ordinary readers but only with appropriate equipment. The second term 'mimicking' defines the action of infiltrating incorrect data into the RFID system. To show an example, the location might be used for authentication of items. By mimicking a tag, the location can be manipulated and items might appear where they do not exist in reality. Fourthly, 'recognition of objects' represents another possible threat of RFID systems. In particular, when persons have been detected, they can be used to explore customer habits. Or, in case of patients who wear implants, these might be recognized and the medical information stored on each implant might be abused. In general, each person who carries objects with affixed RFID tags, like wristwatches, shoes etc. might be recognized by an attacker. Next, the possibility 'tracking of objects' should be considered carefully since tracking of persons can cause many privacy violations. Henrici distinguishes two types of tracking: The first one is called 'direct mapping' and refers to the tracking of RFID wristwatches or glasses. 'Direct mapping' is only possible when the distance between detector and tag is short and the do not exist many tags in one place. Failing that, other items might be tracked by detecting their constellations to each other. These constellations can lead to unwanted creation of movement profiles and the abuse of infrastructure for surveillance by a totalitarian government. Lastly, Henrici defines the threat of 'causing malfunction' which means that attackers (after having abused one of the above mentioned possibilities) are able to render RFID system malfunctioning. This malfuncionting can be revealed by physical destruction or chemical treatment of tags.

3.1.4.2.- Solutions and Methods against Threats

First of all, data security should always be maintained by the RFID system. But what are the exact countermeasures to prevent an attack on an existing RFID system? When Henrici [2, p.64 ff.] talks about solutions and methods against security threats, he calls them 'Goals of Security and Privacy'. In his book, these goals refer to the possible attacks or threats mentioned in section 'Security Problems and Threats' 39. In the following, the countermeasures will be explained. 'Illegitimate reading of data' can be prevented by controlling data access and ensuring data integrity in RFID systems. False data should be infiltrated because of illegitimate access. 'Eavesdropping of data' can be coped with implementing means for detection and recovering so that the system should keep running even if attackers try to put it out of service. Besides, the integrity of system should always be kept. Another strategy preventing eavesdropping is to maintain data security. Henrici defines a 'good' RFID system to be able to cope with illegitimate reading of data and to treat all the data confidentially. 'Cloning or mimicking of tags' which can be compared to counterfeiting can be prevented by using authenticity mechanisms to identify specific tags. Therefore, RFID tags that can prove their own authenticity should be preferred. Unwanted 'recognition of objects' can be avoided by developing technical models that provide suitable trade-off of functions. If a function is not wanted by the user, e.g. to allow everyone in the surroundings to read out all RFID attached object, he can adjust this by defining different user roles and rights.

Regarding the realization of the above mentioned goals, there exist many challenges which have to be faced. Henrici [2, p.66 ff.] describes four general challenges which will be explained in the following paragraph. First of all, since there are different parties, like e.g. logistic companies and customers which have different needs, the developer has to meet all of their requirements. For instance, the different user needs might be realized by developing different views which depend on the particular user role. Secondly, developing a secure RFID system is a multidisciplinary challenge [2] including six different departments: Computer science (designing communication protocols and the middleware), electrical engineering (realizing the required functionality in hardware and

physical layer of communication between tags and readers), mathematics (developing basic cryptographic primitives and theory of probabilities for different areas), economics (adapting the application's constraints imposed by laws of market and assessing real world applicability of approaches), social sciences (including user's requirements, such as privacy and usability) and law (maintaining a legislative basis among people and organizations). Thirdly, there are more requirements to be faced than 'only' security and privacy, such as low costs or coping with few capabilities and resources. Besides, the enrollment of an RFID system, e.g. in a hospital with many distinctive departments, leads to an inter-organizational operation. To implement this inter-organizational operation, several standards have to be integrated. Last but not least, additional requirements have to be considered: Scalability of the system, dependability, low complexity of system, robustness, transparency and usability etc. Henrici claims, that the safeguards should not limit the read range and the speed of reading. Moreover, when using cryptographic primitives, migration paths should be considered.

3.1.5.- State of the Art

There exist many companies which develop Radio Frequency Identification (RFID) solutions and applications. In this paragraph, three important medical companies which provide RFID solutions, will be presented.

3.1.5.1.- Dipole Company

To start with the first company, in the following, the spanish company 'Dipole' [9] will be depicted. 'Dipole RFID' was found in Barcelona 20 years ago with the aim of developing systems for intelligent identification, data capture and systems integration. In their product scope, Dipole provides three main products. The first product contains RFID as well as NFC solutions which should improve optimizing processes, realizing industry 4.0 and the IoT. The second product consists in manufacturing RFID tags to measure the according user needs of Dipole's users. The third product is composed of consulting services, RFID software and systems integration. In their section 'RFID Hospital and Health', Dipole mentions some use cases for their RFID

solutions. To give an example, the correct administration of banked blood can be controlled by using RFID tags. Or, when product stock or termination date of medication and drugs in a hospital have to be observed, RFID tags provide a simple and large-scale use instead of controlling the stock manually (which also brings the risk of human errors). For broader use in hospitals, such as managing whole buildings and improving their workflows, RFID solutions should be considered as well. There exist many hospitals which administrate their workflows with paper-based solutions. As a consequence, the processes are getting very slow and data is duplicated. Furthermore, the communication between several departments is flawed and causes further problems. Another health service, provided by Dipole, is the 'Traceability of Analysis'. In a hospital or a healthcare institution, there are many processes which embody information about clinical analysis, blood tests and blood preservation. These information are very important for patient's diagnosis and treatment. In a laboratory, all tissue samples are stored and several cultivation processes have to be controlled. To increase efficiency of these processes, establishing a RFID system to track and identify all samples correctly would be a useful solution. When it comes to the management of buildings and workflows, the asset tracking forms an important part. Dipole distinguishes two different classifications of assets: Reusable Transport Items (RTI) and products of high value, e.g. elements from the IT and mobile machines. The second type of elements needs specific control in real-time. For an appropriate tracking of IT elements it should be possible to locate each item in a global and detail view to be sure that it is settled in the correct place and under the right conditions, such as the correct temperature or low air humidity. Another use case is guaranteeing the correct dosage of medication to patients which is very important for patient's health and and the work of nursing staff. To simplify the dosage of medication to each patient, RFID tags can be sticked to the pill cases to ensure the correct distribution in real-time. Concerning the management of patients, it is possible to track patients indiviually by wearing bracelets which contain a RFID tag. Currently, the tracking of persons is very controversial because the patient's privacy is offended by enabling his persecution. On the other side, RFID bracelets enable to register patient's actions in real-time and ensure their safety. For example, if a patient suffers from epilepsy, it is dificult to predict an epileptic shock. But if he wore a bracelet which constantly synchronizes

his health status with the system, doctors would be able to act preventively against such shocks and could minimize his risk to die of his illness. Not only managing whole buildings is important but also the tracking and control of material in the operating rooms plays a significant role. For instance, in operating room A exists a mobile Computer Tomograph (CT) whereas operating room B only has set of instruments for surgery. When there is a emergency and the patient needs a CT because the doctor cannot say if he needs the suggested operation but in the operating room B does not exist a CT, it is necessary to detect the next mobile CT rapidly and not to deteriorate the patient's health status.

3.1.5.2.- Cardinal Health Inc.

Cardinal Health Inc., with its headquarters in Dublin and Ohio, founded 100 years ago, [10] is a global company which provides integrated healthcare services and products. There exist four product fields in the scope of Cardinal Health Inc.: logistics, caring of patients, business solutions, and guidance of patients. Cardinal Health Inc. provides Inventory Management Solutions [11] which are specialized on hospital's inventory. In a promotional video, they quote different types of inventory systems, such as the '2-Bin-Kanban' system which is adapted for low cost items needing right sizing and bulk level. A second inventory system which provides management for low cost items needing oversight at the each level is the 'Barcode' system. For high value implantables and physician preference items, the company advertises RFID as best used technology. In the video [11], they claim that reading RFID tags is fast, e.g. 100 tags can be read in seconds. Moreover, RFID tags implicate ease of use for users and support user's needs very quickly. The physician does not have to care about the data capture of his observation because all RFID tagged items are automatically tracked and the measured data is captured by backend interfaces which synchronize to other IT systems (like Materials Management System or Billing Systems). In addition to that, automatic data capture avoids redundant data entries, provides errors and saves time. Another important fact about RFID technology is its accuracy and uniqueness. Cardinal Healthcare Inc. advertises that RFID applications enable automated real-time tracking at a unique item level. Beyond, these applications provide a pro-active

management of expired and recalled products. As a result, RFID applications lead to a streamlined workflow in which charges are automatically captured for accurate billing and compliants as well as clinical documentation are supported. All in all, Cardinal Health Inc. claims that by using its Inventory Management Solution for hospitals will enable physicians and nurses to focus more on patient care and spend less time on managing supplies [11].

3.1.5.3.- Terso Solutions Inc.

Terso Solutions Inc., formed in 2005 in Madison (Wisconsin, U.S.), is specialized on RFID product development and provides several RAdio Frequency IdentificatioN (RAIN) RFID solutions. RAIN RFID [12] is a wireless technology which enables the wireless connection of items to the internet. As a global alliance, RAIN RFID promotes the universal adoption of UHF RFID technology which can be compared to the WiFi Alliance. RAIN uses a standardized GS1 UHF Gen2 protocol to connect all members (network, software, readers, tags, items) of its solution. However, Terso Solutions Inc. has developed a solution for Medical Field Inventory Tracking which prevents a wide range of services to hospitals. In a promo [13], the company shows its solution which connects the RFID technology to medical field by integrating RFID into the medical kit. By using this Medical Field Inventory Tracking, sales can be instantly recorded, field inventories and reverse overstock situations can be run. Besides, automated inventory reporting is possible which brings the side benefit of eliminating shipping costs. Each wrap can be located by the system and the closest needed device is shown. The advantages that accrued are better handled recalls, eliminated overnight shipping demands and reduced expired products. All in all, Terso Solutions Inc. provides two large RFID applications: The 'RFID for Compliance and Product Integrity' and the 'RFID for Compliance and Implant Tracking' which have also been approved for case studies in two hospitals in the U.S.. The first hospital where Terso Solutions Inc. performed its 'TrackCore' case study was the North Kansas City Hospital. RAIN RFID-enabled intelligent cabinets, integrated with TrackCore Inc.'s tissue and implant tracking software as well as the 'TrackCore Operating Room' were tested. Furthermore, 'Jetstream', a cloud-based platform from Terso was proved at 'North Kansas City

Hospital'. The second case study was implemented at St. Dominic Hospital. The tested application included Terso's autoated tissue and implant tracking solution using RFID.

3.1.5.4.- Vizinex RFID

Vizinex RFID was founded in 2012 and is located in Bethlehem, Pennsylvania, U.S. Specialized on the development of RFID tags, Vizinex provides tracking, security and authentication solutions which are based on the RFID technology. Concerning RFID, the company mentions several use cases of the technology [8] which will be mentioned in the following. Firstly, RFID can be used to detect counterfeited drugs. Secondly, the company suggests the use of RFID in the medical equipment field by establishing real time locating systems. As an example, hospital staff is able to rapidly locate critical medical devices, defibrillators. As a positive consequence, Vizinex remarks the enhancement of patient's safety and the reduction of investments in equipment which are needed [8]. Another use case is the inventory management (see also Cardinal Health Inc. 44) and tracking of consumables used in an operation (like for example scalpels, sponges, clamps or surgical equipment). The last point (tracking of consumables in an operation) indicates that after each operation everything can be automatically accounted for. In respect of the use for patients, Vizinex instruct ID cards, wrist or ankle bands and labels which can be attached to patients records. The company declares these identification possibility as a great aid to ensure that the right procedures and medications are applied (see Chapter 1, Internal Communication 3). Regarding the possibility of patient tracking, Vizinex brings up patients with afflictions such as Alzheimer's disease which makes it very difficult to live securely alone. For that reason, tracking people which suffer from Alzheimer within a facility can improve and avoid the risks of getting lost or entering an area where these people might harm themselves. In regard to laboratories, Vizinex names the following examples. The RFID technology can be used to track tissue or fluid samples. While samples are moved through various preparation steps there can occur several errors from data entry or mishandling which can be avoided by automatic tracking. Consequently, the samples that arrive at the pathologist for analysis will automatically contain the related patient record. Besides,

an indication can be called to the computer screen to ensure the proper association of the sample with the patient. As another example, Vizinex depict RFID uses for the discovery of drugs. Especially valuable assets are difficult to inventory but it is essential to do this with a high level of accuracy. All in all, there exist many use cases for the RFID technology. Nevertheless, the use of this technology brings up some concern related to the confidentiality of medical information [8]. Vizinex calls RFID tags 'licence plates' for the items they tag because only the identification number is contained on the tag whereas all 'human readable' information (such as the asset, drug, tissue sample or patient) resides in a database. The FDA highly recommends the external storage of confidential and private patient data and proposes an outline of three components for ensuring medical information security [8]. First of all, all information should be kept confidential. Secondly, the data should be accurate and complete. Thirdly, the data should be available and accessible. To realize the third component, the information should be store on a computer based system. By maintaining these provisions, data entry errors will be reduced, work and information flows will be automated, asset and consumable inventories will be improved and the association of treatment plans with patients will be improved.

4. Development of Medication Tracking Application

4.1.- Used platforms and technologies

4.1.1.- Native Development with NativeScript

There exist several ways to create a mobile application. But the challenge is to develop a consistent solution for the existing systems, like e.g. Android or iOS. To face the challenge of developing both an Android and iOS application, one has to think of the usage of web development technologies, like for example HTML5, CSS and Javascript. These technologies provide the advantage of using the access to browser/internet connection.

editor for writing simultaneously apps at one moment (both for Android and iOS devices)

4.1.2.- NoSQL Technology: MongoDB

4.1.2.1.- Characteristics of NoSQL Databases

4.1.2.2.- Reasons and Advantages of MongoDB

strong consistency and atomicity secondary indexes ad hoc queries querying/indexing/updating similar to relative databases (like SQL/Microsoft Access)

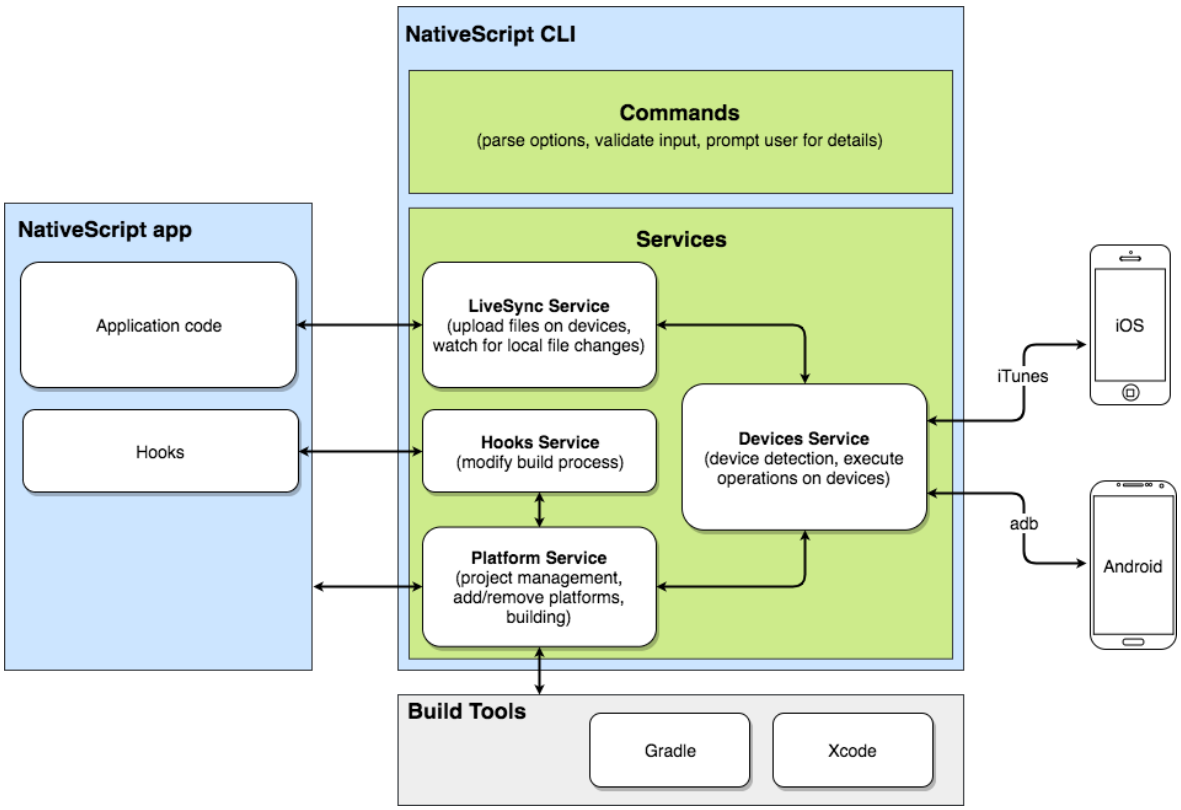


Figure 4.1.- The architecture of NativeScript Applications [14]

4.1.3.- Impinj RFID Lector and Antenna

4.1.3.1.- General Information

4.1.3.2.- Examples

4.2.- Application development

4.2.1.- Challenges during development

Mongodb integration within nativescript application –¿ with Node JS package installer but synchronization with data from Mongodb was difficult

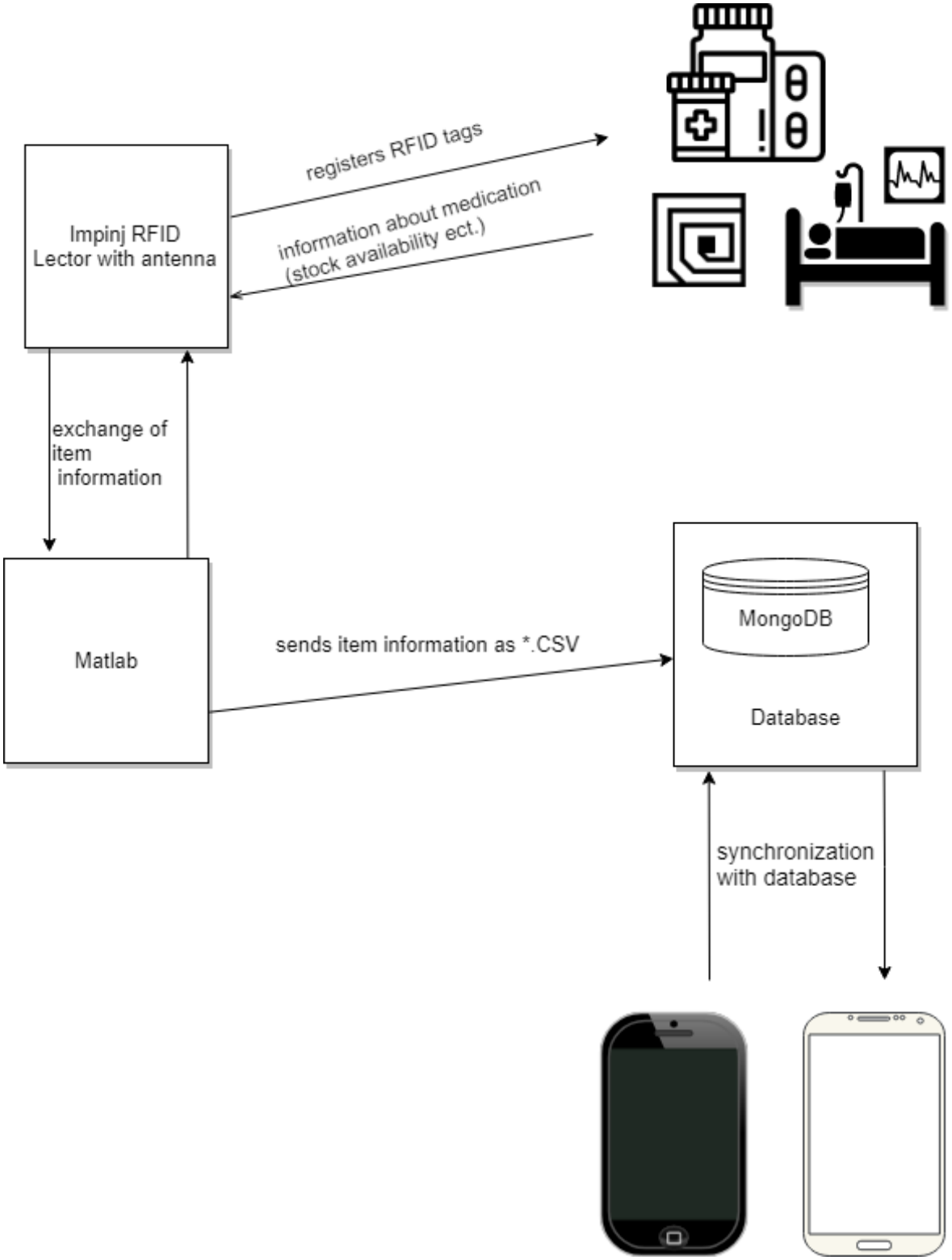


Figure 4.2.- The developed system architecture of the mobile RFID application

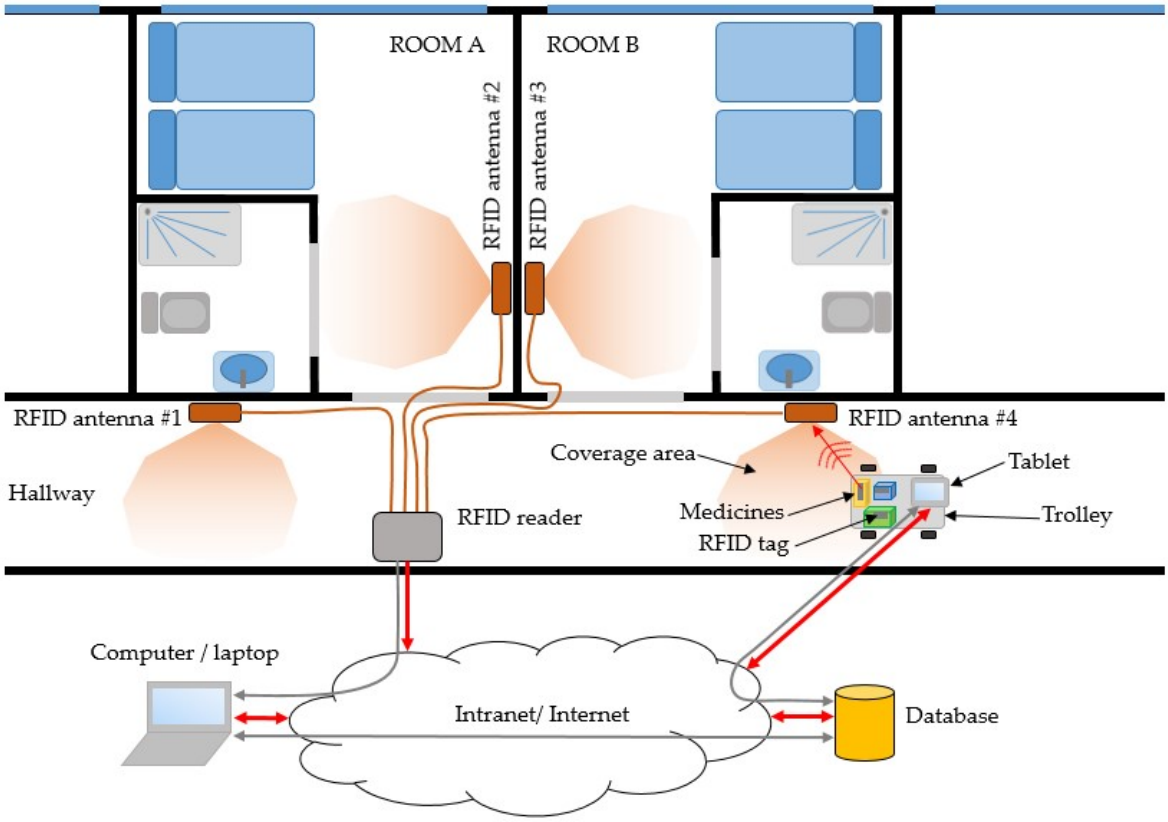


Figure 4.3.- Application scenario of RFID application

4.2.2.- Progress of development

4.2.2.1.- User Scenario

4.2.2.2.- Software Architecture

picture of general software architecture: 2 antennas, 1 lector (RFID Impinj), Database (MongoDB), GUI: Android and iOS Application

4.2.3.- Possibilities of extension

Henrici [2, p.121 ff.] describes four alternative channels to authenticate and authorized the right tags and to prevent attacks on RFID applications. The first possibility of an alternative channel is to use written text to authenticate special operations, for instance on packaging. The master key can be printed on the interior of the product package and is proposed as key recovery mechanism. Furthermore, optical barcodes

can be used together with RFID to ensure identification of items. Especially barcodes attached to each item can be used for general identification of objects. Additionally, RFID tags might be used to assign items of high value. A third possibility of using side channels is to use optical input, such as photodiodes attached to RFID tags. Each RFID tag can use flashes of light (also called optical channel) to transfer data. Lastly, a physical contact channel can also be used alternatively. Compared to smartcards, this methods defends against wireless sabotage or denial of service attacks.

Bibliography

Bibliography

[1] S. Ajami and A. Rajabzadeh, "Radio frequency identification (RFID) technology and patient safety", *J Res Med Sci*, vol. 18, no. 9, pp. 809–813, Sep. 2013. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3872592/ (visited on 03/12/2018).

[2] D. Henrici, *RFID security and privacy: concepts, protocols, and architectures*, ser. Lecture notes electrical engineering 17. Berlin: Springer, 2008, 269 pp., OCLC: 244058698.

[3] G. Tamm and C. Tribowski, *RFID*, ser. Informatik im Fokus. Berlin: Springer, 2010, 144 pp., OCLC: 845690868.

[4] S.-W. Wang, W.-H. Chen, C.-S. Ong, L. Liu, and Y.-W. Chuang, *RFID Application in Hospitals: A Case Study on a Demonstration RFID Project in a Taiwan Hospital*. 2006, vol. 8, 184a–184a. DOI: 10.1109/HICSS.2006.422.

[5] M. Chen and S. Chen, *RFID Technologies for Internet of Things*, ser. Wireless Networks. Cham: Springer International Publishing, 2016. DOI: 10.1007/978-3-319-47355-0. [Online]. Available: http://link.springer.com/10.1007/978-3-319-47355-0 (visited on 03/13/2018).

[6] *Mobile Computing und RFID im Facility Management*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008. DOI: 10.1007/978-3-540-77552-2. [Online]. Available: http://link.springer.com/10.1007/978-3-540-77552-2 (visited on 03/13/2018).

[7] R. Rezaiesarlak and M. Manteghi, *Chipless RFID*. Cham: Springer International Publishing, 2015. DOI: 10.1007/978-3-319-10169-9. [Online]. Available: http://link.springer.com/10.1007/978-3-319-10169-9 (visited on 03/13/2018).

[8] (Feb. 19, 2010). Medical uses for RFID products, Vizinex RFID, [Online]. Available: https://www.vizinexrfid.com/medical-uses-for-rfid-products/ (visited on 03/07/2018).

[9] (Mar. 7, 2018). Rfid hospital sanidad — dipole, [Online]. Available: http://www.dipolerfid.es/es/RFID-Hospital-Sanidad (visited on 03/07/2018).

[10] (Mar. 27, 2018). Cardinal health: Healthcare solutions, logistics supplies, [Online]. Available: http://www.cardinalhealth.com/en.html (visited on 03/27/2018).

[11] (Apr. 15, 2016). Considering RFID to track healthcare inventory?, DAIC, [Online]. Available: https://www.dicardiology.com/videos/considering-rfid-track-healthcare-inventory (visited on 03/07/2018).

[12] (Feb. 11, 2018). RAIN RFID, RAIN RFID, [Online]. Available: https://rainrfid.org/ (visited on 02/11/2018).

[13] Terso Rfid, *RFID for medical field inventory tracking*. [Online]. Available: https://www.youtube.com/watch?v=-G9XNpuH8iQ (visited on 03/12/2018).

[14] *Nativescript-cli: Command-line interface for building NativeScript apps*, original-date: 2014-06-30T10:21:20Z, Mar. 7, 2018. [Online]. Available: https://github.com/NativeScript/nativescript-cli (visited on 03/08/2018).

RFID Radio Frequency Identification

NFC Near Field Communication

IoT Internet of Things

CT Computer Tomograph

RTI Reusable Transport Items

IT Information Technology

UHF Ultra High Frequency

RAIN RAdio Frequency IdentificatioN

HIS Hospital Information System

RIS Radiology Information System

LIS Laboratory Information System

EPC Electronic Product Code

WORM Write Once Read Many

WARD Wisely Aware RFID Dosage

MIMS Mobile Intelligent Medical System

LF Low Frequency

HF High Frequency

UHF Ultra High Frequency

SSL Secure Sockets Layer

TLS Transport Layer Security

FDA Federal Drug Administration

SMLE Single Logical Message Exchange

SARS Severe Acute Respiratory Syndrome

LBMS Location-based Medical Service

TMUH Taipei Medical University Hospital

ERP Enterprise Resource Planning

HL7 Health Level 7

DICOM Digital Imaging and Communications in Medicine

IoT Internet of Things

CATS Compact Approximator based Tag Searching protocol

ITSP Iterative Tag Search Protocol

VHF Very High Frequency

RCS Radio Communication System

UWB Ultra Wide-Band

FMCW Frequency-Modulated Continuous Wave

SNR signal-to-noise

TDR time-domain reflectometry-based

SAW surface acoustic wave

CMT characteristic mode theory

SEM singularity expansion method

TOA time of arrival

MF matched filter

SOA Service-oriented architecture

WLAN wireless local area network

IrDA	Infrared Data Association
PC	Personal Computer
SOAP	Simple Object Access Protocol
API	Application's Programming Interface
WfMS	Workflow-Management System
ASP	application-service-provider
ESB	Enterprise Service Bus
SWOT	Strengths Weaknesses Opportunities Threats
CEP	Complex Event Processing
SME	Small and Medium-sized enterprises