hochschule mannheim

Development of a mobile application with the technology of RFID for managing drugs in hospitals and pharmacies

Jacqueline Franßen

Bachelor Thesis

for the acquisition of the academic degree Bachelor of Science (B.Sc.)

Course of Studies: Medical Informatics

Department of Computer Science

University of Applied Sciences Mannheim

31.08.2018

Tutors

Prof. Dr. Miriam Föller-Nord, Hochschule Mannheim

Prof. Dr. Thomas Smits, Hochschule Mannheim

Franßen, Jacqueline:
Development of a mobile application with the technology of RFID for managing drugs in hospitals and pharmacies / Jacqueline Franßen. –
Bachelor Thesis, Mannheim: University of Applied Sciences Mannheim, 2018. 25 pages.

Franßen, Jacqueline:
Entwicklung einer mobilen RFID-Anwendung zum Arznei-Management in Krankenhäusern und Apotheken / Jacqueline Franßen. –
Bachelor-Thesis, Mannheim: Hochschule Mannheim, 2018. 25 Seiten.

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Ich bin damit einverstanden, dass meine Arbeit veröffentlicht wird, d. h. dass die Arbeit elektronisch gespeichert, in andere Formate konvertiert, auf den Servern der Hochschule Mannheim öffentlich zugänglich gemacht und über das Internet verbreitet werden darf.

Mannheim, 31.08.2018

Jacqueline Franßen

Abstract

Development of a mobile application with the technology of RFID for managing drugs in hospitals and pharmacies

The following thesis is focussed on the development of an mobile hybride application which can be run on Android as well as on 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.

Entwicklung einer mobilen RFID-Anwendung zum Arznei-Management in Krankenhäusern und Apotheken

In der folgenden Arbeit wird die Entwicklung einer mobilen, hybriden Anwendung für Android- und iOS-Smartphones beschrieben. Die Anwendung wurde für den Einsatz in Krankenhäusern und Apotheken entwickelt. Das User-Szenario beinhaltet die Erfassung, Verfolgung und Verwaltung von medizinischen Arzneimitteln und Medikamenten, welche mittels der RFID-Technologie realisiert wurde.

Contents

Chapter 1

Use of RFID Technology

The following chapter will discuss the reasons why choosing the technology and the scope of the RFID technology. It will start by explaining fundamental information and functionalities of RFID readers, tags and further equipment to build a RFID application. After that, some 'State of the Art' applications and use cases will be shown. In the end, there will be mentioned some large companies which provide medical RFID solutions.

1.1. Motivation

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

1.1.1. 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. For instance, RFID tags which are equipped with sensors to ensure the effectiveness of medicine accelerate 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.

1.1.2. Internal Communication

Secondly, poor communication between nurses and physicians deteriorates medical supply. For instance, if a nurse notices that a patient needs a more tranquilizer because he became very nervous, she has to tell the doctor to dose the patient with the correct amount of tranquilizer. But often, a physician is occupying another patient. So, the communication is one problem but the other problem is the staff shortage. Thus, inadequate patient monitoring is emerges. And sometimes, there is the risk of misidentification of patients. To explain the last point, there is an 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.

1.1.3. 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 should 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 mentions 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.

1.1.4. 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 medication medicine. There exists multiple intents of developing a 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 application of RFID technology to specimen bottles was started. The aim of this initiative was to create a paperless pathology requisition system and the correct confirmation by both the endoscopy nursing staff as well as the endoscopist for each specimen bottle. As a result of deploying the application, specimen-labeling errors were significantly reduced.

1.1.5. 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 integrated barcode and RFID tags which should demonstrate effective and safe patient care environment. To give another example of RFID applications, 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]. The mobile application MIMS 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 with other HIS.

1.1.6. RFID applications in hospitals: A case study

In their conference paper, Wang et al. [3] describe a case study of implementing a RFID system in a Taiwan hospital in the year 2003. The project that was studied was named Location-based Medical Service (LBMS) and was performed in the Taipei Medical University Hospital (TMUH). In the following section, the development strategy, device management as well as the value generation which are important for developing RFID applications in healthcare organizations, will be discussed. 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/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 in 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) [3, 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 wanted to build a system that could detect and track potential SARS cases. 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 relevant personnel via 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 legitimate drug control. Wang

et al. were supported by the Taiwanese government which approved their plan and granted money. As 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 [3, p.4] which consisted of professors emerging technology and making 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 [3, 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 [3, 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. All in all, 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 occur intermittent and unreliable reads. These might 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 [3, p.2 ff.], Wang et al. depict some existing RFID applications. To give an example of a succesful 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. depict applications for tracking and managing equipment such as wheelchairs, 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 of serial numbers might be a challenge which could be coped with setting a primary key to each tag which synchronizes with an existing database (see Chapter 3, 'Used platforms and technologies' 23. The third challenge is to deal with the real-time data and to synchronize it seasonably. To deal with the third challenge, the use of NoSQL databases makes sense and will be discussed in Chapter 3 24.

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 [3, p.7]. In addition to that, the authors claim 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 [3].

1.2. 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 20). Inventory Management is significant for managing 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.

1.2.1. 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. [4, p.2 f.] depict smart applications and a specific problem which they call 'tag search problem'. The problem 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 [4, 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 a anonymous RFID authentication mecha-

nism 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 give limited hardware resources. To face the problem of limited hardware resources, Chen et al. suggest an 'asymmetric design principle' [4, 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 [4, p.4 f.]. To give an example, in large warehouses there exist 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 network leads to worst-case energy costs which should be avoided.

To avoid the above mentioned energy costs, resulting from inefficient protocols, Chen et al. describe several tag searching protocols [4, 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 it polling problem. The idea of CATS is to encode the tag IDs into a 'Bloom' filter [1] [4, p.15] and to transmit the Bloom filter instead of the ID. Consequently, in the first phase of CATS, the

[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.

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 tags in the coverage area. Each tag receives its Bloom filter and tests whether it belongs to set X. Unwanted tags will be kept silent 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 busy slot which means that at least one tag is transmitting whereas '0' stands for 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.

Chapter 2

General Information about RFID technology

2.1. 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.

2.1.1. 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 has to be an antenna which detects each tag and creates a magnetic field. The antenna is connected to its reader which receives the tag's information and is able to manipulate tags. 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 a application software, such as a database or user interface.

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. In contrast, the 'Auto-id' systems imply the automatic identification of its objects. Generally spoken, RFID systems can be seen as a subset of 'Auto-id' systems.

When it comes to the variety of RFID tags, three fundamental types are distinguished: Active, semi-active and passive RFID tags [2] which all constist 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 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 complexe and secure method to identify tags which is called 'multistep identification' is described by Henrici. As the name of this method is very self-explaining, one has to think of 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 tranmission of 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, it would be no additional expenditure to enable encrypted and shared key identification of tags using passive tags.

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 and 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. To give an example of the use of stationary readers, they can be used for goods receiving or stock management. Furthermore, stationary readers are fixed to a specific location and need permanent network connection. On the opposite, mobile readers do not need permanent network connection and are used for querying prices in a supermarket. As mentioned in the section before 12, 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. 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 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.

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 processing is moved from tags into middleware so that tags only have to identify objects. As a result, modularity of the system is maintained.

Concerning the data management of RFID systems, 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].

2.1.2. Functionality of RFID system

First of all, 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].

2.1.3. 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' 17, five important recommended countermeasures will be described.

Security Problems and Threats

As Henrici [2] mentions, there exist two fundamental fears about the RFID technology. The first fear concerning 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 vi-

olated 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 12, 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' 14, 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.

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' 15. 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.

2.1.4. 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.

Dipole Company

To start with the first company, in the following, the spanish company 'Dipole' [5] 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 Near Field Communication (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.

Cardinal Health Inc.

Cardinal Health Inc., with its headquarters in Dublin and Ohio, founded 100 years ago, [6] 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 [7] 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 [7], 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 [7].

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 [8] 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 [9], 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.

2.1.5. Examples

Chapter 3

Development of Medication Tracking Application

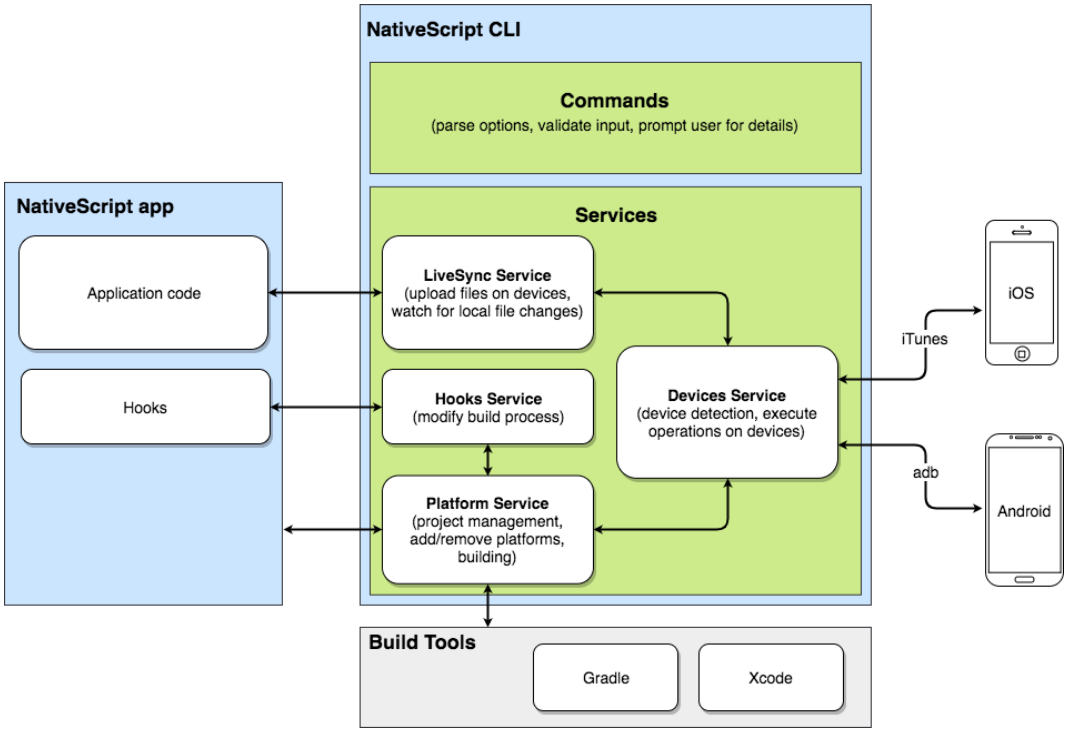
3.1. Used platforms and technologies

3.1.1. 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.

NativeScript Sidekick

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



The architecture of NativeScript Applications

Figure 3.1.: The adopted from [10]

3.1.2. NoSQL Technology: MongoDB

Characteristics of NoSQL Databases

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)

3.1.3. Impinj RFID Lector and Antenna

General Information

Examples

3.2. Application development

3.2.1. Challenges during development

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

3.2.2. Progress of development

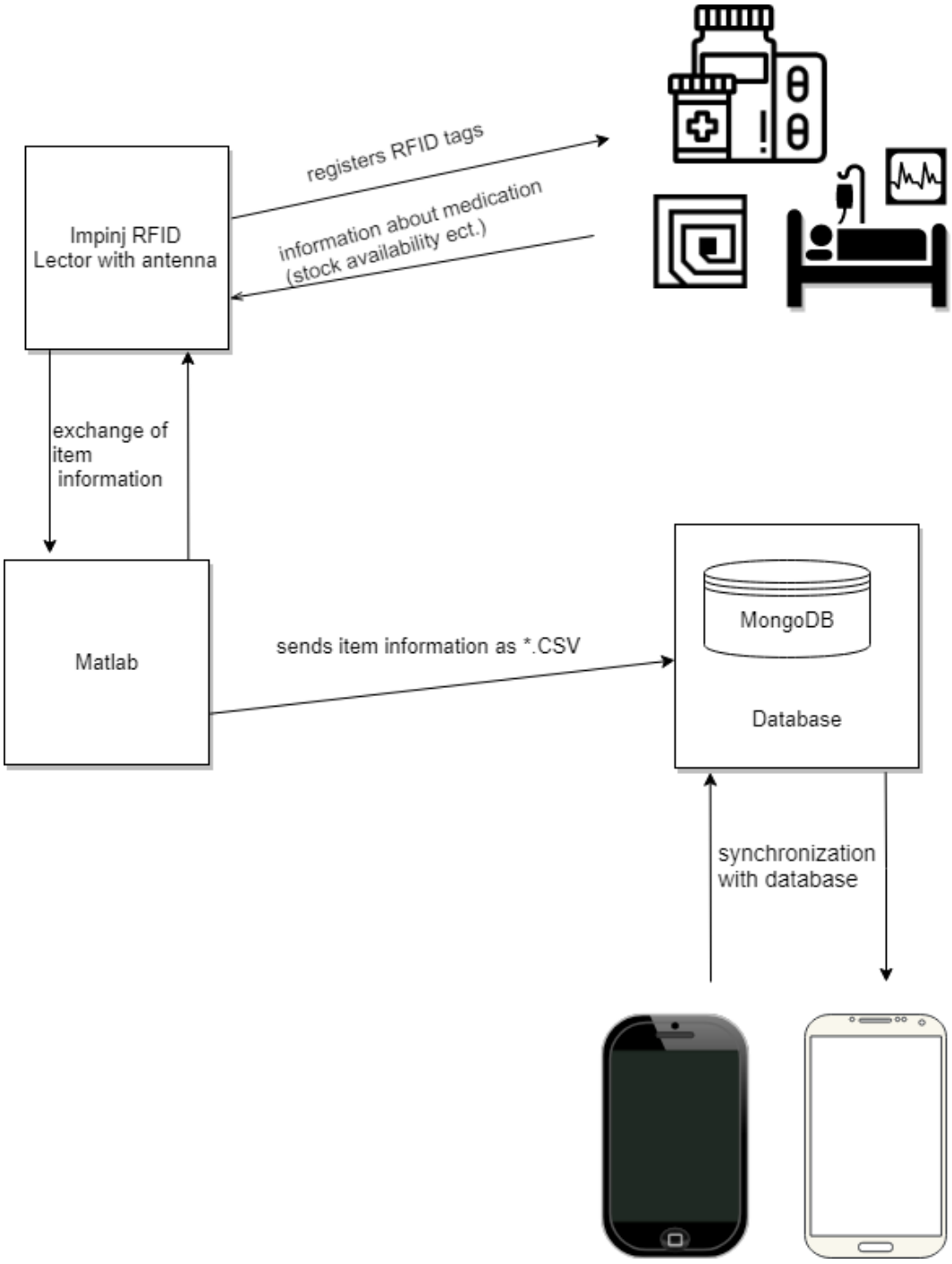
User Scenario

Software Architecture

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

3.2.3. 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.



The developed system architecture of the mobile RFID application

Figure 3.2.

List of Abbreviations

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

List of Tables

List of Figures

Listings

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] 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.

[4] 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).

[5] (Mar. 7, 2018). RFID Hospital Sanidad | Dipole, [Online]. Available: http://www.dipolerfid.es/es/RFID-Hospital-Sanidad (visited on 03/07/2018).

[6] (Mar. 27, 2018). Cardinal Health: Healthcare Solutions, Logistics Supplies, [Online]. Available: http://www.cardinalhealth.com/en.html (visited on 03/27/2018).

[7] (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).

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

[9] Terso Rfid, *RFID for Medical Field Inventory Tracking*. [Online]. Available: https://www.youtube.com/watch?v=-G9XNpuH8iQ (visited on 03/12/2018).

[10] *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).

Appendix A

Erster Anhang

Hier ein Beispiel für einen Anhang. Der Anhang kann genauso in Kapitel und Unterkapitel unterteilt werden, wie die anderen Teile der Arbeit auch.

Appendix B

Zweiter Anhang

Hier noch ein Beispiel für einen Anhang.