RFID Security in Supply Chains: A Theoretical Analysis, a Case Study and a Simulation Model

Inaugural dissertation submitted by Simon Rihs in fulfillment of the requirements for the degree of Doctor rerum oeconomicarum at the Faculty of Business, Economics and Social Sciences of the University of Bern.

submitted by

Simon Rihs

from Safnern (BE)

2015

The faculty accepted this work as dissertation on 2015-09-17 at the request of the two advisors Prof. em. Dr.Dr.h.c. Gerhard Knolmayer and Prof. Dr. Guido Schryen, without wishing to take a position on the view presented therein

I am grateful for having been supported by many people over the course of my thesis:

My deepest gratitude goes to Prof. em. Dr.Dr.h.c. Gerhard Knolmayer for his valuable input to the research and his patience during the course of preparing this thesis. A special thank you goes to Prof. Dr. Guido Schryen for honoring me in being the co-referee for this thesis.

Thank you to Prof. Dr.-Ing. André Miede for providing the source code of the simulation model and for his valuable input to co-authored paper.

Many thanks go to all my former colleagues at the iwi, for many interesting discussions over coffee and their input – especially Dr. Roman Schmidt and Patrick Sarbach.

To my parents and my sisters, for providing support and casually ignoring the elephant of my unfinished thesis in the room :-)

Finally, a special thank you goes to Dr. Monica Bachmann, without whom this thesis would have never reached a conclusion.

Table of Contents

Abstract

The number of promising applications of Radio Frequency IDentification (RFID) for industry and consumers has risen considerably over the years. There are many advantages in using RFID compared to other identification technologies such as barcodes. For example, direct machine interaction with the physical world is possible, no line-of-sight is required, and higher data density and faster read-rates may be achieved. However, several security and privacy issues have been raised, mostly focusing on privacy issues of the consumer. This thesis focuses on the security issues of RFID within a supply chain and consists of three papers and an umbrella relating the three papers to the state of RFID research. Two of the following three papers have already been published:

- Rihs, S. (2009a). RFID Security Risks in Supply Chains: More than Privacy. *International Journal of Enterprise Network Management.* 3(4), pp. 347 - 357.
- Rihs, S. (2009b). *Lademittelbewirtschaftung mit Hilfe von RFID - Fallstudie bei der Schweizerischen Post*. Universität Bern.
- Rihs, S. and Miede, A. (2014). Discovering Suppliers' Customers by means of Statistical Disclosure Attacks. *International Journal of RFID Security and Cryptography.* 3(1), pp. 148 - 155.

First, a generic risk matrix regarding the use of RFID was designed and analyzed. Open- and closed-loop RFID supply chain setups were analyzed with regard to the impact of different attacks. Furthermore, possible countermeasures against these attacks were outlined. It was shown that eavesdropping and tag injection are the attacks with the highest impact and likelihood in a supply chain environment with shared tags amongst partners in the supply chain (see Section 3).

Second, a study of a very large-scale RFID deployment for the management of package items at the Swiss Post was conducted. Here, special focus was given to the suitability analysis of RFID for this application scenario and the developed software. The risks involved with regard to the RFID data were also examined. In conclusion, both the use of RFID and the developed

software are found to be suitable for this application scenario while the risk of using RFID is low in this case (see Section 4).

Third, a simulation model for the vulnerability of an RFID-equipped supply chain distribution center against an implementation of the statistical disclosure attack (SDA) was developed. The analysis showed that the success probabilities for the statistical disclosure attack vary depending on the structure of the customers, their number as well as on the organization of the distribution center. The probability of success was found to decrease if there are multiple product deliveries to a customer per round. A decrease in success probability is also noticeable if only a fraction of all deliveries are observed. If this fraction falls below a certain threshold, which is determined by the organization of the distribution center, the attack is highly improbable to succeed (see Section 5).

Aspects of RFID security in supply chains were thus analyzed from a theoretical (Section 3), empirical (Section 5), and practical (Section 4) point of view, yielding pertinent results and having impacts both for researchers and practitioners.

1 Introduction

1.1 Background

Fundamentally, every company acquires capital, goods, and services, performs operations on these inputs, and markets the resulting products or services. Companies that coordinate their flow of goods, services, or money in order to gain a competitive advantage are linked in a supply chain. Their coordination is facilitated, among other factors, by better information flow between the companies.[1]

While there are several technologies that can be used to improve supply chain operations, a technology expected to improve information flow within and between companies and that has received heightened attention from academia and practitioners is Radio Frequency IDentifcation (RFID).[2]

RFID is an automated identification technology based on electromagnetic messages exchanged between a sender and a tag (for a brief introduction to RFID, refer to Chapter 2.2). The expected benefits of RFID use have led to an overestimation of market growth by research and practitioners. While the adoption of RFID in supply chains has been slower than initially anticipated[3], there are a growing number of companies in multiple industries that are implementing RFID in their supply chain operations at the palette or item level.[4]

1.2 Problem Description

Since its inception, the adoption of RFID has raised many security concerns, even resulting in boycott calls by consumer rights groups concerning the lack of privacy in early trials.[5] This has led to a wide body of research regarding

[1] Prajogo and Olhager, 2012, pp. 514.

[2] Nativi and Lee, 2012, pp. 366.

[3] Leung et al., 2014, p. 206; Wu et al., 2006, pp. 1317.

[4] N.N., 2014d.

[5] ACLU, 2015.

the privacy issues of RFID.[6] However, much less research has been conducted regarding the security issues prior to the point of sale in supply chains. The application of RFID in security-critical supply chains, such as the defense industry[7] further underscores the necessity for researching RFID security within supply chains.

1.3 Aim of the Thesis

The main motivation for this thesis was to contribute to the body of research within this identified research gap regarding the security implications of RFID usage in a supply chain (prior to the point of sale) leading to the following aim:

The aim of this thesis is to identify and analyze possible security issues due to RFID use in supply chains prior to the point of sale.

This aim has led to the development of the following research questions:

- If and how does the use of RFID change the risk profile for a supply chain?
- What is the security impact of RFID in the use case of package item management?
- Assuming an increased attack surface stemming from RFID use in a distribution center, could traffic analysis be a potentially successful avenue of attack?

In order to analyze these questions, a theoretical analysis, a case study, and a simulation study have been carried out leading to the following three main contributions of this thesis:

[6] Avoine, 2015.

[7] N.N., 2015c.

- The development and analysis of a generic risk matrix regarding the use of RFID in supply chains.[8]
- The description and analysis of, at the time of writing, one of the largest RFID deployments[9] in Switzerland.[10]
- The vulnerability analysis and simulation of a specific traffic analysis attack, the statistical disclosure attack (SDA) against a supply chain distribution center using RFID.[11]

1.4 Structure of the Thesis

This thesis will begin with a brief introduction to supply chains, RFID, and security in information technology. The papers presented in Sections 3, 4, and 5 require a certain degree of prior knowledge with regard to the topics presented in Section 2. All papers are related to the supply chain literature (Section 2.1) as well as to the security of RFID systems (Section 2.4). The latter chapter is based on the topics of RFID (Section 2.2) and information security (Section 2.3). The papers follow the introductory section in their original formatting and language. A summary and outlook are given at the end of this thesis.

[8] Rihs, 2009a.

[9] Swisscom, 2008.

[10] Rihs, 2009b.

[11] Rihs and Miede, 2014.

2 Background Information

This chapter provides a brief overview on supply chains, RFID, and security in information technology (IT).

2.1 Supply Chains

The term supply chain itself can be somewhat misleading, since a supply chain is not only looking at a single supplier or the supply side of an organization, but is taking into account all material, information and monetary flows of the organizations participating in a supply chain[12] (see Figure 1).

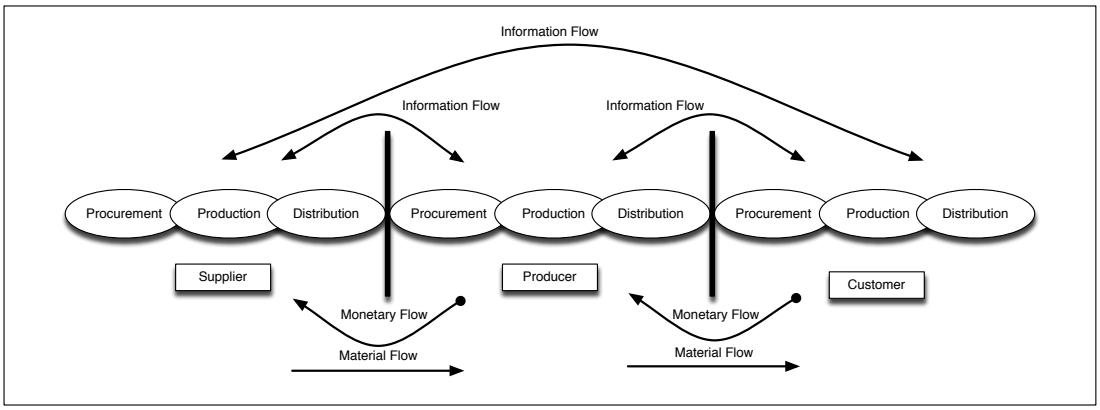


Figure 1: Process view of a supply chain[13]

RFID can contribute to render the information and material flow in a supply chain more efficient. An overview of possible effects of the use of RFID on supply chains follows in Section 2.2.

As this thesis is analyzing RFID security within supply chains (as opposed to consumer privacy), supply chains are at the core of the identified research gap.

[12] Knolmayer et al., 2009, p. 3.

[13] Translated and adapted from Bothe and Nissen, 2003, p. 2; Bartsch and Bickenbach, 2002, p. 25.

2.2 RFID

This section is a short primer on RFID and offers the necessary background information regarding RFID technology and applications for Sections 3, 4 and 5.

2.2.1 Technology

While RFID has gained much attention recently, the underlying technology was already used in 1939 during the Second World War to identify friendly airplanes.[14] In 1948, Stockman described the technology in his article "*Communication by means of reflected power*".[15]

As the title of Stockman's paper suggests, RFID communication is based on using the power of one element to communicate with others. In an RFID system, the reader sends out an electromagnetic or radio signal that is received by the so-called RFID tags. Depending on the frequency, these tags respond to queries from the reader either via inductive coupling or electromagnetic coupling.[16]

A typical RFID system always includes one or multiple tags, one or multiple readers, and one or multiple backend systems. The term "reader" is somewhat misleading, as data can not only be read, but also be written from a reader onto a tag. RFID tags (or transponders or chips) can be classified along multiple dimensions, such as energy, communication distance and frequency, memory, computing power, tamper resistance, physical characteristics, and standards (for some examples of RFID tags, see Figure 2). Tags without their own energy source are called passive tags, which are most widely used in logistical applications.[17]

Near Field Communication (NFC) is related to RFID and uses the same frequency and similar protocols as High Frequency (HF, 13.56 MHz) tags.

[14] Garfinkel et al., 2005, p. 34.

[15] Stockman, 1948.

[16] Cf. Avoine, 2005, pp. 62.

[17] Cf. Avoine, 2005, pp. 62.

The communication of NFC distance is limited to a few centimeters, and there are numerous consumer applications planned.[18]

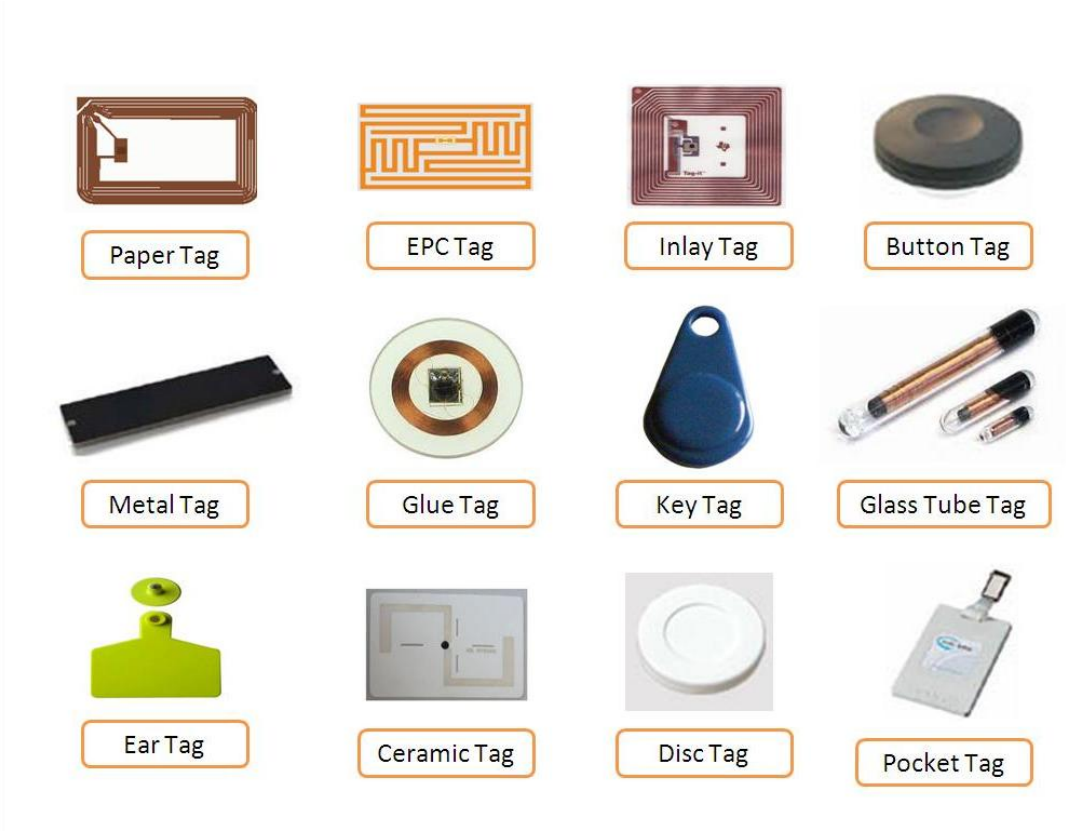


Figure 2: Different kinds of RFID tags[19]

The ongoing miniaturization of tags as well as cost reductions have led to broader application possibilities for industry and consumers, which are outlined in the following chapter.

2.2.2 Industry Uses

There are multiple uses of RFID in logistics. In supply chains, RFID has several advantages over more traditional product identification approaches such as barcodes. The main advantage of RFID is to give IT systems awareness of specific objects without requiring human interaction, thus enabling faster data and material flow. A ubiquitous application of RFID and interconnected RFID-systems is known as the "*Internet of Things*", as it links

[18] Cf. Thrasher, 2013; Joan, 2009.

[19] N.N., 2014b.

the physical world and IT. For example, a search engine that retrieves the history and current location of specific objects instead of webpages might be created.[20]

2.2.2.1 Inventory Management

An RFID enabled inventory management system could allow for an almost instantaneous inventory by querying the entire shelf or even warehouse. Smart shelves at the point-of-sale will recognize when a customer removes an item and can automatically require replenishment to avoid out-of-stock situations. RFID can be used in supply chain management for increased information flow amongst partners by sharing location and throughput times amongst partners. The literature as well as literature reviews suggest a positive impact of RFID in supply chain management.[21]

Transponders are not only placed on pallets, containers or boxes, but can be used as a replacement for barcodes to identify individual products. In contrast to barcodes, an RFID tag will not only hold the information to identify a product group, but also give a unique identifier to each and every product. This is referred to as *item-level tagging*.[22]

2.2.2.2 Smart Shops

There have been several applications for RFID-aware shops. The Future Store initiative by METRO in Germany was one of the early testing grounds for the applicability of RFID in retail, which began in the company's prototype shops in 2004.[23]

More recently, Nespresso has begun to implement RFID-based self-service shopping zones in their Nespresso stores with the goals to reduce waiting times and improve customer satisfaction.[24]

---

[20] Eds: Fleisch and Mattern, 2005.

[21] Cf., e.g., Sarac et al., 2010; Sari, 2010; Tajima, 2007.

[22] Zhou, 2009.

[23] N.N., 2013.

[24] N.N., 2014a.

2.2.2.3 Tracking and Tracing

Tracking and tracing are applications which are also facilitated by RFID. *Tracking* refers to following an item's progression downstream through the different stages of a supply chain. The most commonly known use is the possibility to track parcels and shipments of logistics providers (such as the Swiss Post, DHL, FEDEX, UPS, or TNT) on their respective websites. *Tracing* means following the different stages of the supply chain upstream in order to determine the origin of a product or part (e.g., in case of recalls). For instance, there have been several RFID initiatives for tracing food back to its origin in case of contamination.[25]

2.2.2.4 Security as RFID Application

RFID can also be used as a security and anti-counterfeiting measure for expensive items, such as watches or industrial goods.[26]

There have also been suggestions to use RFID as means to ensure that pharmaceutical drugs are genuine and not counterfeited. This can be achieved by providing a fully recorded history of a tagged drug, from the production through transport up to the point-of-sale.[27]

In order to verify the history of a tagged product, there are multiple options. First, a secure record of all read events can be kept on the tag. This requires the tag to include a certain amount of memory with write access, which makes the production of the tag more expensive. Furthermore, the logged events need to be signed by each reader to prevent a forged history (as long as private signing keys are secure). Another option is to keep a record of all sightings of tags in a central database. If a tag suddenly appears in the supply chain or the same tag number appears twice in different locations at the same time, it can be flagged as possibly counterfeit. This option requires a central database or means to correlate data in distributed databases. The

[25] E.g., Piramuthu et al., 2013; Chen et al., 2008; Kelepouris et al., 2007; Regattieri et al., 2007.

[26] Staake et al., 2005.

[27] Cheung and Choi, 2011, p. 710.

two options could also be combined, by having a log both on the tag and in a central database.[28]

The cryptographic signing of tags as proof of a product's origin has also been proposed, as only the genuine manufacturer of a given product should have the private key that is necessary for the signature.[29]

2.2.3 Consumer Uses

Consumer applications of RFID can also be expected to rise as readers and tags become more widespread. With NFC readers now common in high-end smartphones and NFC being planned for a broad range of applications such as advertising, payment services (e.g., Apple Pay), home automation, and education, a further increase in the utilization of this technology is expected.[30] While the application of NFC is recent, there are consumer RFID applications that have been deployed for over 25 years.

2.2.3.1 Transportation

One of the earliest consumer uses of RFID technology was road toll collection, with Norway starting its rollout in 1987. In most electronic toll collection systems, a tag (active or passive) is attached to the front of a vehicle either inside or outside of the vehicle and is read when passing through a set of reading gates. Today, electronic toll collection systems are widely used for road toll systems.[31]

RFID is not only used for the toll collection for private transport, but also for the ticketing services of public transport systems. Travel cards in metropolitan areas, such as the Oyster Card in London or the OV-chipkaart for all public transports in the Netherlands, are now common. Beginning in

[28] Cf. Juels, 2006, p. 384.

[29] Lehtonen et al., 2007, p. 130.

[30] Knoll, 2014.

[31] Landt, 2005, p. 10.

August 2015, an RFID based "*Swisspass*" will replace the formerly used "*GA Travelcard*" and "*Half-Fare Travelcard*" in Switzerland.[32]

2.2.3.2 Home Appliances

Smart home appliances are, at the time of writing, still not widely deployed. The US-based coffee company Keurig has released coffee makers which read RFID tags to change brewing recipes depending on the coffee capsule used.[33] While the new Keurig coffee machines also incorporate a system to limit coffee-making capabilities only to capsules from Keurig, this limitation is currently implemented by means of infrared scanning of the coffee capsule lid and not by RFID.[34]

There have also been applications in washing machines that identify optimal washing cycles for the type of clothing put in them, as well as smart fridges that can identify the dates of expiry on items stored.[35] While both of these applications have been successfully used in industry, they are dependent on the universal implementation of item-level tagging before being useful to the consumer.

Another category of RFID consumer application is healthcare at home, with RFID-enabled smart medical shelves that can recognize when a drug has not been taken on time, as well as monitor a patient's compliance with a doctor's prescription in terms of timing and dosage.[36]

2.2.3.3 Access Control

RFID has also been widely deployed to provide access controls for vehicles and buildings. Most vehicles have an RFID-enabled key that prevents them from being started if a physical key does not have the correct RFID chip. Since 1995, such car immobilizers are required by law for new vehicles sold

[32] N.N., 2015a.

[33] Swedberg, 2012.

[34] Storm, 2014.

[35] Cf., e.g., N.N. 2012; Darianian and Michael, 2008.

[36] Yao et al., 2012.

in the EU. Furthermore, many current vehicles no longer require a key to be inserted into a keyhole to start them. The presence of the key within the vehicle being all that is needed for starting the vehicle.[37]

Many buildings have access systems that are RFID-based, though these often include physical keys as fallbacks or for additional security. RFID-based building access offers the possibility of fine-grained access control over areas without the issues associated with physical key and lock distribution; furthermore, time-delimited access restrictions are also possible (e.g., granting access to server rooms only during maintenance periods).[38]

2.3 Information Security

The safeguard of information against unauthorized or unwanted access or modification is an important aspect of all IT systems. This section offers a brief introduction to the fundamentals of computer security necessary for Sections 3 and 5, for further information several comprehensive textbooks have been written as introductions to computer security.[39]

The three basic components of IT systems are hardware, software, and data. These resources are exposed to risks due to certain vulnerabilities. A vulnerability is a weakness which could be used to cause damages or losses, whereas an attack is the abuse of such a vulnerability. A threat encompasses the possibility of damages or losses. Examples of threats are floods, hackers, or human error when customizing a system.[40]

The difference between vulnerabilities, threats, and attacks can be outlined using the following example of a logistics department:

- Unauthorized access by a third party in the logistics department gaining information about customers and pricing is a threat.

[37] Verdult et al., 2012.

[38] Finkenzeller, 2012, pp. 575.

[39] Cf., e.g., Pfleeger et al., 2015; Eds: Bosworth et al., 2014; Gollmann, 2011.

[40] Cf., e.g., Raggad, 2010, p. 82.

- Underlying vulnerabilities are (amongst countless others) obsolete virus definition files and lack of physical access control to offices of the logistics department.
- An attack in this case could be a gift of free memory sticks infected with a malicious program that transmits the desired shipping and turnover data to the attacker.[41]

When analyzing security systems, a safe assumption is that malicious attackers both always use the best method of attack currently available and have complete knowledge of the attacked system. Therefore, an encryption system should be designed to withstand attacks even given complete knowledge of the system, with exception of the decryption keys. This principle is called Kerckhoffs's principle, named after the second requirement for military encryption postulated by Auguste Kerckhoffs in 1883.[42]

2.3.1 Goals of IT Security

Traditionally, three main security aspects are mentioned in the literature and are referred to as the confidentiality, integrity, and availability (CIA) triad of information security.[43]

Over time, several additions have been proposed for this basic triad of security goals, such as non-repudiation, meaning the undeniability of actions such as viewing or altering a document. Furthermore, authenticity, utility, and possession have also been proposed as fundamental security elements.[44]

2.3.1.1 Confidentiality

Confidentiality means that only authorized persons can access a resource. Unauthorized read access is a breach of confidentiality, as is unauthorized printing, or even the knowledge about the existence of a resource. While the goal of confidentiality is easily understandable, the definition of authorized

[41] Johnston, 2010, pp. 31.

[42] Kerckhoffs, 1883, p.12.

[43] Raggad, 2010, p. 20.

[44] Cf., e.g., Pfleeger et al., 2015, p. 36; Parker, 2014, p. 110; Gollmann, 2011, p. 34.

access to a system can become very complicated.[45]

An example of loss of confidentiality is industrial espionage. The motivation for industrial espionage is to obtain confidential information from or about a competitor in order to gain a competitive advantage. Industrial espionage is also sometimes attributed to nation-states in order to boost their national industrial capabilities, especially in the defense and energy industries. Due to the importance and ubiquity of IT systems in businesses and the pertinence of information contained within them, IT is an increasingly important target.[46]

2.3.1.2 Integrity

Integrity is more difficult to define than confidentiality, as it can mean a multitude of things, including precise, error-free, unchanged, changed only through an authorized process, consistent, and correct, among others. In this context, integrity implies that a resource remains unchanged unless it is changed by authorized persons or by an authorized process.[47]

An example for loss of integrity could be the malicious editing of payment information in an accounting system, such as shifting all account numbers to the next supplier in a database.

Another example of integrity loss is a Microsoft Word macro virus that maliciously inserts the word "*not*" into texts after certain instances of the word "*is*". While such texts remained grammatically correct (rendering detection more difficult), the meanings of these altered texts are completely changed.[48]

[45] Cf., e.g., Pfleeger et al., 2015, pp. 37; Parker, 2014, p. 114.

[46] Connolly, 2009.

[47] Cf., e.g., Pfleeger et al., 2015, p. 39; Parker, 2014, p. 113.

[48] Pfleeger et al., 2015, p. 39.

2.3.1.3 Availability

Availability means that authorized persons can access the required resource. The presence of a given resource, the required capacity, the acceptable waiting time, and adequate response times are all part of the notion of availability.[49]

A common example of availability loss is Internet downtime due to problems with a user's router or with a service provider's infrastructure.

As shown in Figure 3, these three goals (confidentiality, integrity, availability) can overlap and even contradict one another. For instance, very high confidentiality can impact availability by making time-intensive cryptography necessary.

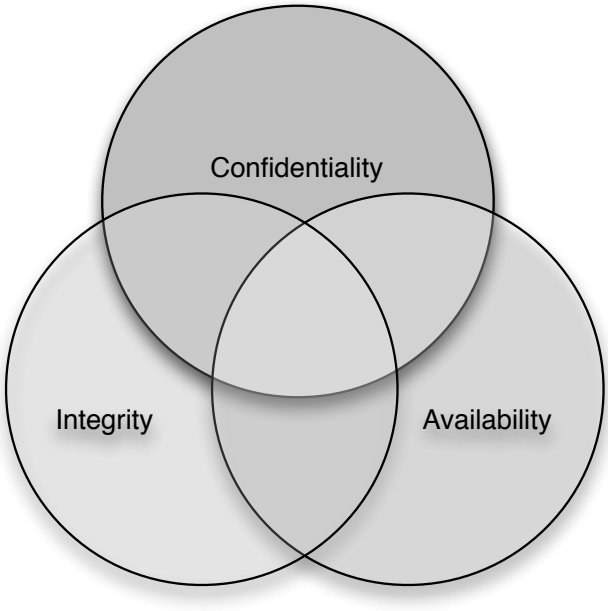


Figure 3: Interdependency between confidentiality, integrity, and availability[50]

The following threats impede these goals of information security.

[49] Pfleeger et al., 2015, p. 45; Parker, 2014, p. 112.

[50] Kennedy, 2009.

2.3.2 Threats

Any security threat can be classified into one or into a combination of the following four classes. Note that each of the threat classes can apply to one or to all of the IT components (i.e., hardware, software, and data).[51]

2.3.2.1 Interruption

An interruption means that hardware, software, or data is lost, unusable, or unavailable. As the legitimate users are denied access to a resource, the security goal of availability is violated. Examples of interruptions include denial of service attacks against a webpage or the loss of backup tapes.[52]

2.3.2.2 Interception

If an unauthorized party has gained (read) access to data, hardware, or software, there has been an interception. A person or a program can carry out an interception; for example, an employee could copy data and transfer it to a third party, or a program could redirect network packages. All these actions result in a breach of confidentiality. It is important to note that an interception does not necessarily result in an interruption for the legitimate users. [53]

Another class of attacks based on interception are disclosure attacks, such as the statistical disclosure attack discussed in detail in the third publication of this thesis (Section 5).[54]

2.3.2.3 Modification

A modification involves the unauthorized access with the goal to make changes, resulting in a breach of integrity. Data can be changed in a database or programs could be modified as described earlier (Section

[51] Cf. Pfleeger et al., 2015, p. 47.

[52] Cf. Pfleeger et al., 2015, p. 47.

[53] Cf. Pfleeger et al., 2015, p. 47.

[54] Rihs and Miede, 2014.

2.3.1.2). The modification of hardware is also possible, such as removing memory from the server. [55]

2.3.2.4 Creation

Creation involves the unauthorized entry of new data, software, or hardware in a system, which leads to a loss of integrity.[56] For example, a new invoice could be entered into an accounting system, or hardware elements, such as a device to capture user input, could be integrated into a system.

The above-mentioned threats can stem from the following different sources:[57]

- Abusers (criminal) and misusers (negligence)
- Accidental occurrences (failure of hardware or software)
- Environmental influences

Due to this variety of sources, security analysis should not solely focus on a single source, as this could lead to flawed conclusions e.g., only focusing on criminal activities while analyzing an underground data center in a flood-prone area.

2.3.3 Controls

Controls (or countermeasures) should counter threats and prevent vulnerabilities from being exploited for an attack. Controls can have preventive, deterring, deflecting, mitigating, detecting, or recovering properties (or a combination thereof) to counter threats. Table 1 gives an overview of the types of control and their meaning.[58]

[55] Cf. Pfleeger et al., 2015 p. 47.

[56] Cf. Pfleeger et al., 2015 p. 47.

[57] Parker, 2014, p. 110.

[58] Cf. Pfleeger et al., 2015 p. 57.

Table 1: Control types and their meaning[59]

Control	**Meaning**
Preventive	Completely blocking the attack or closing the vulnerability
Deterring	Making the attack more difficult but not impossible
Deflecting	Making other targets more attractive (or comparatively lowering the attractiveness of oneself for attacks)
Mitigating	Reducing the impact of the attack (e.g., by limiting its reach)
Detecting	Detecting attacks in real-time or later (e.g., IT Audits)
Recovering	Actions that help to recover from attacks

As controls are always implemented on a certain layer of an IT system, it is important to note that attacks on a lower layer than the layer of the control are still possible, which in turn renders defense on an upper layer difficult. If an attacker has control of the operating system on a computer, he can usually modify the security properties of applications running on the computer.[60]

2.4 Security of RFID Systems

RFID security continues to be a field of active research. The “RFID Security and Privacy Lounge” webpage, which is maintained by the Information Security Group of the *Université Catholique de Louvain* and collects conference proceedings and journal articles regarding RFID security and privacy, lists over 1000 references since 2002. The number of references increased from a single article in 2002 to 127 references in 2013, then

[59] Cf. Pfleeger et al., 2015 p. 57.

[60] Gollmann, 2011, p. 45.

dropping to 85 references in 2014.[61] Whether this decrease is just a temporary downturn or an indication of waning research interest in RFID security remains to be seen.

In addition to ongoing research, several organizations have released guidelines that define best security practices for the implementation of RFID projects. The German "Bundesamt für Sicherheit in der Informationstechnik" has published a series of comprehensive guidelines for the use of RFID in different application areas, such as e-ticketing and trade logistics.[62] Furthermore, the American Department of Homeland Security[63] (for the use of RFID in passports), the American National Institute of Standards and Technology,[64] and the Organization for Economic Co-Operation and Development[65] have each published guidelines with emphasis on security and consumer privacy.

2.4.1 Attacking RFID Systems

There are multiple attack vectors for an RFID system. A brief overview such attacks is presented in Table 2. The detailed descriptions of these attacks as well as the rationale for their classification are given in Section 3.[66] As the threats against an IT system (see Section 2.3.2) are also applicable to RFID systems, the threat type as well as the violated security goal are also listed in Table 2.

As it is the case for the controls discussed in the previous chapter, an attack against an RFID system occurs on different layers of an RFID system. The layers of an RFID system are the physical layer, the protocol layer, and the application layer.[67]

---

[61] Avoine, 2015.

[62] Bartels et al., 2009.

[63] DHS, 2006.

[64] Karygiannis et al., 2007.

[65] OECD, 2008.

[66] Rihs, 2009a.

[67] Avoine and Oechslin, 2005, p. 115.

Table 2: Overview of attacks and their layer[68]

Layer	Type of Attack	Threat	Violation of
Application Layer	Injection	Modification / Creation	Integrity
Protocol Layer	Timing Attacks	Interception	Integrity, Confidentiality
	Denial of Service	Interruption	Availability
	Eavesdropping	Interception	Confidentiality
	Injection	Modification / Creation	Integrity
Physical Layer	Electromagnetic Pulse	Interruption	Availability
	Injection	Modification / Creation	Integrity

It is important to note that the SDA, which is discussed in detail in the paper[69] Section 5, is primarily based on eavesdropping. Eavesdropping was identified as main risk in open-loop RFID supply chains within the paper[70] presented in Section 3.

However, the expected likelihood of an SDA is lower than that of a simple eavesdropping attack, as such an attack is more complex and requires more effort from the attacker. Carrying out an SDA against an existing distribution center would only be sensible if the target is hardened against eavesdropping e.g., with a pseudonym scheme (presented in Section 2.4.2.7), thus necessitating a more sophisticated attack.

In the following section, possible countermeasures against RFID attacks will be outlined.

[68] Based on Rihs, 2009a, p. 351.

[69] Rihs and Miede, 2014.

[70] Rihs, 2009a, p. 353.

2.4.2 Securing RFID Systems

The following countermeasures are ordered by the layer in which they can be implemented (see Table 3), beginning with the lowest layer (physical layer).

2.4.2.1 Kill Instruction

The “Kill” command was introduced by EPC-Global to counter the fears regarding the lack of privacy of consumers. There are two kinds of kill commands; a soft kill ensures that a tag no longer sends out a serial number, but only a short manufacturing identification. A hard kill physically destroys the tag.

The “killing” of tags has certain drawbacks, as customers can no longer benefit from the information capabilities of a tag. Home applications such as intelligent appliances like an intelligent medical cabinet, which could be very useful for elderly consumers, would no longer be functional once the tags are killed. Furthermore, in case of a soft kill, an RFID-profile of a person can still be created if the person carries or wears enough tags.[71]

For applications within a supply chain, killing is completely unsuitable, as the tags will no longer be functioning, and thus, preventing any use of the RFID information within the supply chain.

Juels has suggested to use the kill command as an authentication mechanism. This is based on the fact that a killing requires more energy than normal communication. If a reader sends out a kill command with insufficient energy, the tag reacts with the message that the password was correct, but that it was sent with too little energy. If the password of the tag has not been compromised, the reader has authenticated the tag.[72]

2.4.2.2 Tag-Clipping

An approach closely related to the kill command is the clipping of the tag. The chip is physically separated from the antenna by tearing off a strip that

[71] Garfinkel et al., 2005, p. 39.

[72] Juels, 2005, pp. 7

connects the antenna and the chip. This is visible to the naked eye and ensures that RFID communication is no longer possible. If the functionality of the tag needs to be restored, for example, to handle refunds at the point-of-sale, its contacts can be bridged, resulting in a functional tag.[73]

Similar to killing, this approach is more suitable for consumers than for applications within a supply chain due to the requirement for manual intervention.

2.4.2.3 Blocker-Tags

The underlying idea of the blocker-tag is not to harden the individual tags against attacks, but to create a hostile environment for (rogue) RFID readers. The corresponding communication frequencies are flooded with information in order to prevent a reader from establishing communication with a tag. A blocker-tag requires an energy source and is more expensive than passive tags. As only one blocker-tag is needed for each securable zone (e.g., person or container), cost is less of an issue in large-scale deployments compared to other countermeasures that require implementation on every tag.[74]

The use of a blocker-tag is best suited to secure transports between participants of a supply chain.

Alternatively to having a single blocker-tag flooding communication channels, another possible countermeasure to secure against traffic analysis (as outlined in Section 5) would be to have a large random number of additional RFID tags (“Dummy Tags”) which are not connected to a specific physical item. This renders gaining information about the transported items more difficult, as it is impossible for an attacker to determine if a tag is attached to an item or not without an optical check.

[73] Karjoth and Moskowitz, 2005.

[74] Garfinkel et al., 2005, p. 40.

2.4.2.4 Encryption

While encryption would appear to be a prime candidate for a countermeasure against the above-mentioned threats, certain issues need to be taken into account. The secure distribution of encryption and decryption keys in complex RFID systems is difficult, as you need to ensure that all legitimate users of the tag have access to the necessary decryption keys. In some cases (such as passports) it is possible to print the decryption keys on the item, which requires an optical scan prior to the RFID communication. This approach is not sensible for supply chains, as the RFID tags should replace the need for optical scanning.[75]

Furthermore, an encrypted serial number is still a static identifier, which means it can be tracked just as easily as an unencrypted one, with the encrypted identifier acting as a meta-identity. Lastly, while dynamic encryptions could be implemented on more expensive tags, in applications with numerous tags, Moore's law[76] will be overcompensated by cost pressures.[77]

2.4.2.5 Fallback Scenario

In case of a successful disruption attack against an RFID system, a fallback scenario reduces the impact of the attack as it allows processes to continue. Examples of possible fallbacks are barcodes or manual data entry. While such fallback procedures allow for the continuous use of the system, the additional effort they require reduces the effectiveness of the system. However, a fallback scenario is still less costly than a total shutdown (i.e., no deliveries of products), as it mitigates the effect of an attack and helps to recover from it.[78]

[75] Cf. Garfinkel et al., 2005, p. 39.

[76] Moore's law refers to the prediction in 1965 by Intel founder Gordon Moore that a processors calculating capacity would double every two years. N.N., 2015b.

[77] Cf. Garfinkel et al., 2005, p. 39.

[78] Karygiannis et al., 2007, p. 5-9.

As the RFID system for package items analyzed in Section 4 has a complete fallback scenario with barcodes in place, the total risk of the RFID use in this scenario is greatly reduced.

2.4.2.6 Passwords

Passwords also seem a possibility to counter certain of the above-mentioned threats. The implementation of password-protection is possible on very simple tags, meaning that an RFID tag will only send out information if it receives the correct password. Unfortunately, this leads to a paradox in which the sender cannot know which password to send out without knowing the identity of the tag. Passwords may be able to better secure products in the transport phase between participants of the supply chain, however this also necessitates complex password management strategies.[79]

2.4.2.7 Pseudonyms

If an RFID tag sends out a constantly changing pseudonym instead of a static identifier, some of the threats can be countered.

Ohkubo, Suzuki, and Kinoshita were the first to describe a pseudonym protocol in detail.[80] However, the complexity of this protocol leads to prohibitively high computing costs in large environments, which limits its practical application. While a time-memory trade off has been created to reduce the complexity, it however results in an increased memory demand at the backend.[81]

A tree-based pseudonym protocol has been proposed that accounts for the ownership transfer of tags. The scalability is dependent on the branching factor of the underlying tree and can be adapted to the implemented

[79] Cf. Garfinkel et al., 2005, p. 39.

[80] Ohkubo et al., 2003.

[81] Avoine et al., 2005.

scenario.[82] However, at low branching levels, the security of the protocol is degraded due to the shared keys within a branch.[83]

The SDA discussed in Section 5 is based on the assumption of strong on-tag security, e.g., with a well-designed pseudonym protocol on the tags.

2.4.2.8 Silent Tags

The silent tag is a commercially available solution in which a queried tag only responds to queries with the correct identifier.[84]

Cryptographically, this corresponds to a challenge-response mechanism, with both the challenge and the response sent in the clear. The drawbacks of this solution are similar to a conventional password system, as an RFID reader requires prior knowledge of the location of its tags. An attacker could also gain knowledge of all the identifiers if he prevents a response from the queried tags, as this could potentially force the reader to sequentially send out all identifiers in the system to receive a response.

2.4.2.9 Physical Security

A possible countermeasure to render attacks against RFID systems more difficult is through the implementation and enhancement of physical security measures. Possible security measures include access restrictions within sensitive areas or video surveillance as detection measures.[85]

Note that, while physical security has technical elements, its implementation generally occurs outside of an RFID system itself, and is thus listed in Table 3 as a non-technical option.

[82] Molnar et al., 2006, p. 286.

[83] Avoine et al., 2005, pp. 6.

[84] N.N., 2014c.

[85] Karygiannis et al., 2007, p. 5-5.

In Section 3, physical security was noted as one of the primary countermeasures to prevent RFID attacks.[86]

2.4.2.10 Regulatory Options

A non-technical approach to address some problems that arise with RFID use could be regulatory options. Several authors have proposed regulatory approaches to safeguard the privacy of the consumers.[87]

However, for problems within the supply chain, regulatory options do not seem to be suitable, as most of the mentioned threats (such as industrial espionage or sabotage) are illegal.

Table 3 presents an overview of the presented countermeasures against RFID attacks, the layers in which they can be implemented, as well as the type of control.

Table 3: Overview of defense mechanisms and their layer

Layer	Type of Countermeasure	Type of Control
Non-Technical	Physical Security	Detecting, Preventive, Deterring
	Regulatory Options	Deterring
Application Layer	Encryption	Preventive, Deterring
	Fallback Scenario	Mitigating, Recovering
Protocol Layer	Blocker Tags / Dummy Tags	Preventive, Deterring
	Encryption	Preventive, Deterring
	Passwords	Preventive, Deterring
	Pseudonyms	Preventive, Deterring
	Silent Tags	Preventive, Deterring
Physical Layer	Kill Command	Preventive
	Tag Clipping	Preventive

As noted in Chapter 2.3.3, a countermeasure on a higher layer can often be circumvented by an attack on a lower layer.

[86] Rihs, 2009a, p. 354.

[87] Cf., e.g., Spiekermann and Ziekow, 2005; McCullagh, 2003; Garfinkel, 2002.

After outlining the research context of supply chains, RFID, IT security, and RFID security, the research focus of the papers will be presented in the next section.

2.5 Research Focus

A large part of the existing RFID security research is focused on consumer security and privacy, with many papers designing and analyzing protocols. Rather than to examine technical implementations, the three papers that follow this introductory section focus on the threats against and vulnerabilities of entire RFID systems within supply chains. They have the following research focus.

Section 3 discusses and categorizes attacks against supply chains with RFID systems. Two generic risk matrices for supply chains are developed based on the impact and determined likelihood of such attacks. This paper extends the existing literature regarding RFID supply chain risks by offering the possibility to systematically assess RFID risks in supply chains using these risk matrices.

Section 4 is an analysis of a large-scale RFID application scenario involving package items. While the risk matrices in Section 3 were developed for an entire supply chain, this paper analyses an RFID implementation within a single logistics provider. The unique contribution of this paper is a suitability and risk analysis of the largest RFID deployment in Switzerland at the time, leading to generalizable insights for other similar cases.

In Section 5, a simulation model is adapted to simulate an SDA against a single logistics provider, namely a distribution center of a supply chain. This attack scenario is based on the assumption of a distribution center with high security standards (e.g., tags with a pseudonym scheme). It provides lower bounds for security in a given setting. This article is, to the best of the author’s knowledge, the first to assess the consequences of an SDA against RFID systems, and thus to assess the conditions in which RFID systems are particularly vulnerable to network traffic analysis attacks.

After this brief introduction to supply chains, RFID, and IT, the published paper regarding the security risks of RFID in supply chains will be presented in its original formatting in Section 3.

List of Abbreviations – Chapters 1 and 2

ACLU American Civil Liberties Union
BSI Bundesamt für Sicherheit in der Informationstechnik
CIA Confidentiality, Integrity, Availability
DoS Denial of Service
EMP Electromagnetic Pulse
EPC Electronic Product Code
EU European Union
HF High Frequency
IT Information Technology
MHz Mega Hertz
NFC Near Field Communication
RFID Radio Frequency Identification
SDA Statistical Disclosure Attack
US United States

References – Chapters 1 and 2

ACLU. (2015). *RFID Position Statement*. American Civil Liberties Union. [Online] Available from: https://www.aclu.org/national-security/rfid-position-statement. [Accessed: 2015-03-08].

Avoine, G. (2005). *Cryptography in Radio Frequency Identification and Fair Exchange Protocols*. École polytechnique fédérale de Lausanne. [Online] Available from: http://sites.uclouvain.be/security/download/papers/Avoine-2005-thesis.pdf. [Accessed: 2015-01-19].

Avoine, G., Dysli, E. and Oechslin, P. (2006). Reducing Time Complexity in RFID Systems. *Selected Areas in Cryptography*. pp. 291 - 306.

Avoine, G. and Oechslin, P. (2005). RFID Traceability: A Multilayer Problem. *Financial Cryptography and Data Security*. [Online] pp. 125 - 140. Available from: http://link.springer.com/content/pdf/10.1007%2F11507840_14.pdf. [Accessed: 2015-06-14].

Avoine, G. (2015). *RFID Security & Privacy Lounge*. Université catholique de Louvain. [Online] Available from: http://www.avoine.net/rfid/. [Accessed: 2015-05-12].

Bartels, C., Kelter, H., Oberweis, R. and Rosenberg, B. (2009). *TR 03126-4: Einsatzgebiet „Handelslogistik". Technische Richtlinie für den sicheren RFID-Einsatz*. Bundesamt für Sicherheit in der Informationstechnik. [Online] Available from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03126/BSI-TR-03126-4_pdf.pdf?__blob=publicationFile. [Accessed: 2015-05-11].

Bartsch, H. and Bickenbach, P. (2002). *Supply Chain Management mit SAP APO*. 2nd Ed. Bonn: Galileo Press GmbH.

Bosworth, S., Kabay, M. E. and Whyne, E. (eds.) (2014). *Computer Security Handbook*. 6th Ed. Hoboken: John Wiley & Sons.

Bothe, M. and Nissen, V. (2003). *SAP APO in der Praxis*. Wiesbaden: Springer.

Chen, R.-S., Chen, C., Yeh, K., Chen, Y. and Kuo, C. (2008). Using RFID technology in food produce traceability. *WSEAS Transactions on information science and applications.* 5(11), pp. 1551 - 1560.

Cheung, H. H. and Choi, S. H. (2011). Implementation issues in RFID-based anti-counterfeiting systems. *Computers in Industry.* 62(7), pp. 708 - 718.

Connolly, K. (2009). *Germany accuses China of industrial espionage*. Guardian. [Online] Available from: http://www.guardian.co.uk/world/2009/jul/22/germany-china-industrial-espionage. [Accessed: 2015-03-08].

Darianian, M. and Michael, M. P. (2008). Smart home mobile RFID-based Internet-of-Things systems and services. *International Conference on Advanced Computer Theory and Engineering*. [Online] Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4736933. [Accessed: 2015-06-14].

DHS. (2006). *RFID Security and Privacy White Paper*. Department of Homeland Security. [Online] Available from: https://www.dhs.gov/xlibrary/assets/foia/US-VISIT_RFIDattachE.pdf. [Accessed: 2015-05-11].

Finkenzeller, K. (2012). *RFID-Handbuch, Grundlagen und praktische Anwendungen von Transpondern, kontaktlosen Chipkarten und NFC*. 6th Ed. München: Carl Hanser Verlag.

Garfinkel, S. (2002). *An RFID Bill of Rights*. Technology Review. [Online] Available from: http://www.technologyreview.com/articles/02/10/garfinkel1002.asp. [Accessed: 2015-03-09].

Garfinkel, S., Juels, A. and Pappu, R. (2005). RFID Privacy: An Overview of Problems and Proposed Solutions. *IEEE Security and Privacy.* 3(3), pp. 34 - 43.

Gollmann, D. (2011). *Computer Security*. 3rd Ed. Chichester: John Wiley & Sons.

Fleisch, E. and Mattern, F. (eds.) (2005). *Das Internet der Dinge*. Berlin: Springer.

Joan, B. (2009). *Difference between RFID and NFC*. [Online] Available from: http://www.differencebetween.net/technology/difference-between-rfid-and-nfc/. [Accessed: 2015-03-10].

Johnston, R. G. (2010). Being Vulnerable to the Threat of Confusing Threats with Vulnerabilities. *Journal of Physical Security.* 4(2), pp. 30 - 34.

Juels, A. (2005). *Strengthening EPC Tags Against Cloning*. [Online] Available from: http://www.arijuels.com/wp-content/uploads/2013/09/J05d.pdf. [Accessed: 2015-03-09].

Juels, A. (2006). RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications.* 24(2), pp. 381 - 394.

Karjoth, G. and Moskowitz, P. (2005). *Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced*. IBM. [Online] Available from: http://domino.watson.ibm.com/library/cyberdig.nsf/papers/D25E54DB29DAA9AA8525707C00702C9F/$File/rc23710.pdf. [Accessed: 2015-03-08].

Karygiannis, T., Eydt, B., Barber, G., Bunn, L. and Phillips, T. (2007). *Guidelines for Securing Radio Frequency Identification (RFID) Systems*. National Institute of Standards and Technology. [Online] Available from: http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf. [Accessed: 2015-05-11].

Kelepouris, T., Pramatari, K. and Doukidis, G. (2007). RFID-enabled traceability in the food supply chain. *Industrial Management & Data Systems.* 107(2), pp. 183 - 200.

Kennedy, J. M. (2009). *The Information Security triad: CIA. Second version*. [Online] Available from: http://commons.wikimedia.org/wiki/File:CIAJMK1209.png. [Accessed: 2015-03-08].

Kerckhoffs, A. (1883). La cryptographie militaire. *Journal des sciences militaires.* [Online] 9, pp. 5 - 38. Available from: http://www.petitcolas.net/kerckhoffs/crypto_militaire_1.pdf. [Accessed: 2015-05-11].

Knoll, M. (2014). *18 Creative & Useful Ways To Use NFC Tags With Your Smartphone – 2014 Update*. Trendblog. [Online] Available from:

http://trendblog.net/creative-and-useful-ways-to-use-nfc-tags-with-your-smartphone/. [Accessed: 2015-03-10].

Knolmayer, G., Mertens, P., Zeier, A. and Dickersbach, J. (2009). *Supply Chain Management Based on SAP Systems: Architecture and Planning Processes*. Berlin: Springer.

Landt, J. (2005). The history of RFID. *IEEE Potentials*. 24(4), pp. 8 - 11.

Lehtonen, M. O., Michahelles, F. and Fleisch, E. (2007). Trust and security in RFID-based product authentication systems. *IEEE Systems Journal*. 1(2), pp. 129 - 144.

Leung, J., Cheung, W. and Chu, S.-C. (2014). Aligning RFID applications with supply chain strategies. *Information & Management.* 51(2), pp. 260 - 269.

McCullagh, D. (2003). *Are spy chips set to go commercial?* Zdnet. [Online] Available from: http://www.zdnet.com/article/are-spy-chips-set-to-go-commercial/. [Accessed: 2015-03-08].

Molnar, D., Soppera, A. and Wagner, D. (2006). A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags. *Selected Areas in Cryptography*. [Online] pp. 276 - 290. Available from: http://link.springer.com/content/pdf/10.1007%2F11693383_19.pdf. [Accessed: 2015-03-08].

N.N. (2012). *RFID- and NFC-Enabled Smart Washing Machine Detects Fabric, Supports Remote Maintenance*. NXP. [Online] Available from: http://www.nxp.com/news/press-releases/2012/02/rfid-and-nfc-enabled-smart-washing-machine-detects-dabric--supports-remote-maintenance.html. [Accessed: 2015-03-16].

N.N. (2013). *Geschichte der Future Store Initiative*. Metro. [Online] Available from: http://www.future-store.org/internet/site/ts_fsi/node/387810/Lde/index.html. [Accessed: 2015-03-16].

N.N. (2014a). *Champs-Élysées boutique reopens with enhanced design and services*. Nestle. [Online] Available from: http://www.nestle-nespresso.com/newsandfeatures/champs-elysees-nespresso-flagship-boutique-reopens-with-enhanced-design-and-services-. [Accessed: 2015-03-14].

N.N. (2014b). *RFID Tags for Solar Module*. Coresonant. [Online] Available from: http://www.coresonant.com/html/rfid-tags-for-solar-module-india.html. [Accessed: 2015-02-28].

N.N. (2014c). *Secure electronic tags*. Friendly Technologies. [Online] Available from: http://www.friendlytechnologies.com/index.php/our-technology/secure-electronic-tags. [Accessed: 2015-03-20].

N.N. (2014d). Survey: *Use of item-level RFID growing, but slowly*. Supply Chain Quarterly. [Online] Available from: http://www.supplychainquarterly.com/news/20140424-survey-use-of-item-level-rfid-slow-but-growing/. [Accessed: 2015-03-09].

N.N. (2015a). *Die öV-Karte heisst «SwissPass» und wird zusätzlichen Kundennutzen bieten*. Verband öffentlicher Verkehr. [Online] Available from: http://www.voev.ch/de/Medien/Mediendetails?newsid=43. [Accessed: 2015-03-10].

N.N. (2015b). *Moore's Law*. [Online] Available from: http://www.mooreslaw.org/. [Accessed: 2015-04-28].

N.N. (2015c). *RFID in Defense*. RFID Journal. [Online] Available from: http://www.rfidjournal.com/defense. [Accessed: 2015-03-08].

Nativi, J. J. and Lee, S. (2012). Impact of RFID information-sharing strategies on a decentralized supply chain with reverse logistics operations. *International Journal of Production Economics.* 136(2), pp. 366 - 377.

OECD. (2008). *RFID Policy Guidance*. Organization for Economic Cooperation and Development. [Online] Available from: http://www.oecd.org/sti/ieconomy/40892347.pdf. [Accessed: 2015-05-11].

Ohkubo, M., Suzuki, K. and Kinoshita, S. (2003). *Cryptographic approach to "privacy-friendly" tags*, *RFID Privacy Workshop*. Massachusetts Institute of Technology. [Online] Available from: http://rfidprivacy.media.mit.edu/2003/papers/ohkubo.pdf. [Accessed: 2015-03-16].

Parker, D. B. (2014). Toward a New Framework for Information Security. pp. 109 - 131. In Bosworth, S., Kabay, M. E. and Whyne, E. (eds.). *Computer Security Handbook*. 6th Ed. Hoboken: John Wiley & Sons.

Pfleeger, C. P., Pfleeger, S. L. and Margulies, J. (2015). S*ecurity in Computing*. 5th Ed. Upper Saddle River: Prentice Hall.

Piramuthu, S., Farahani, P. and Grunow, M. (2013). RFID-generated traceability for contaminated product recall in perishable food supply networks. *European Journal of Operational Research.* 225(2), pp. 253 - 262.

Prajogo, D. and Olhager, J. (2012). Supply chain integration and performance: The effects of long-term relationships, information technology and sharing, and logistics integration. *International Journal of Production Economics.* 135(1), pp. 514 - 522.

Raggad, B. G. (2010). *Information Security Management: Concepts and Practice*. Boca Raton: CRC Press.

Regattieri, A., Gamberi, M. and Manzini, R. (2007). Traceability of food products: General framework and experimental evidence. *Journal of Food Engineering.* 81(2), pp. 347 - 356.

Rihs, S. (2009a). RFID Security Risks in Supply Chains: More than Privacy. *International Journal of Enterprise Network Management.* 3(4), pp. 347 - 357.

Rihs, S. (2009b). *Lademittelbewirtschaftung mit Hilfe von RFID - Fallstudie bei der Schweizerischen Post*. Universität Bern.

Rihs S. and Miede, A. (2014). Discovering Suppliers' Customers by means of Statistical Disclosure Attacks. *International Journal of RFID Security and Cryptography.* 3(1), pp. 148 - 155.

Sarac, A., Absi, N. and Dauzère-Pérès, S. (2010). A literature review on the impact of RFID technologies on supply chain management. *International Journal of Production Economics.* 128(1), pp. 77 - 95.

Sari, K. (2010). Exploring the Impacts of Radio Frequency Identification (RFID) Technology on Supply Chain Performance. *European Journal of Operational Research.* 207(1), pp. 174 - 183.

Spiekermann, S. and Ziekow, H. (2005). RFID: a 7-point plan to ensure privacy. *Proceedings of the 13th European Conference on Information Systems*. ECIS. [Online] Available from:

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=761047. [Accessed: 2015-03-16].

Staake, T., Thiesse, F. and Fleisch, E. (2005). Extending the EPC network: the potential of RFID in anti-counterfeiting. *Proceedings of the 2005 ACM symposium on Applied computing*. Santa Fe. pp. 1607 - 1612. [Online] Available from: http://dl.acm.org/ft_gateway.cfm?id=1067041&ftid=314362&dwn=1&CFID=519265583&CFTOKEN=27448159. [Accessed: 2015-03-16].

Stockman, H. (1948). Communication by Means of Reflected Power. *Proceedings of the IRE.* 36(10), pp. 1196 - 1204.

Storm, D. (2014). *Keurig 2.0 spoofing vulnerability: Hack bypasses coffee DRM, allows brewing of any pod*. [Online] Available from: http://www.computerworld.com/article/2857708/keurig-2-0-spoofing-vulnerability-hack-bypasses-coffee-drm-allows-brewing-of-any-pod.html. [Accessed: 2015-03-16].

Swedberg, C. (2012). *New Keurig Brewer Uses RFID Recipe Tag to Make the Perfect Cup*. [Online] Available from: http://www.rfidjournal.com/articles/pdf?9934. [Accessed: 2015-03-16].

Swisscom. (2008). *Swisscom und Post realisieren das grösste RFID-Projekt der Schweiz*. [Online] Available from: https://www.swisscom.ch/de/about/medien/press-releases/2008/04/20080428_01_RFID.html. [Accessed: 2015-02-27].

Tajima, M. (2007). Strategic Value of RFID in Supply Chain Management. *Journal of Purchasing and Supply Management.* 13(4), pp. 261 - 273.

Thrasher, J. (2013). *RFID vs. NFC: What's the Difference?* [Online] Available from: http://blog.atlasrfidstore.com/rfid-vs-nfc. [Accessed: 2015-03-10].

Verdult, R., Garcia F. D. and Balasch, J. (2012). Gone in 360 seconds: Hijacking with Hitag2. *Proceedings of the 21st USENIX conference on Security symposium.* [Online] Available from: https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final95.pdf. [Accessed: 2015-05-10].

Wu, N. C., Nystrom, M., Lin, T. R. and Yu, H. C. (2006). Challenges to global RFID adoption. *Technovation.* 26(12), pp. 1317 - 1323.

Yao, W., Chu, C.-H. and Li, Z. (2012). The adoption and implementation of RFID technologies in healthcare: a literature review. *Journal of medical systems.* 36(6), pp. 3507 - 3525.

Zhou, W. (2009). RFID and item-level information visibility. *European Journal of Operational Research*. 198(1), pp. 252 - 258.

3 RFID SECURITY RISKS IN SUPPLY CHAINS: MORE THAN PRIVACY

For copyright reasons (no reprints) the original paper is not included. The full reference including the DOI follows.

Rihs, S. (2009a). RFID Security Risks in Supply Chains: More than Privacy. *International Journal of Enterprise Network Management.* 3(4), pp. 347 – 357. http://dx.doi.org/10.1504/ijenm.2009.032484 .

4 Lademittelbewirtschaftung mit Hilfe von RFID

The paper is presented in its original formatting and language below.

Institut für Wirtschaftsinformatik der Universität Bern
Abteilung Information Engineering

Lademittelbewirtschaftung mit Hilfe von RFID

Fallstudie bei der Schweizerischen Post

Simon Rihs

Bern, 2009 / 2015

Diese Fallstudie wurde Mitte 2009 verfasst und stellt den Projektstand zu diesem Zeitpunkt dar. Anfang 2015 fand eine geringfügige Überarbeitung der Fallstudie statt. Dabei wurden insbesondere Quellenangaben aktualisiert sowie eine Präzisierung der zeitlichen Angaben vorgenommen.

Die Angaben in dieser Fallstudie beruhen auf Informationen und Dokumenten der Schweizerischen Post. Besten Dank an Dr. Thierry Gafner von der PostLogistics sowie Adrian Dubach und Dr. Roman Schmidt von der Swiss Post Solutions AG für die Gesprächsbereitschaft und die Bereitstellung von Informationen.

Inhaltsverzeichnis

1 Gegenstand der Fallstudie

Die Schweizerische Post betreibt für den Paketvertrieb eine komplexe Distributionslogistik mit über drei Paketzentren, 31 Distributionsbasen und 20 Distributionsfilialen. Aufgrund der durch die manuelle Bewirtschaftung der 45'000 Rollboxen entstandenen Kosten hat die Post 2008 für die Sicherstellung einer ressourcenschonenden, sicheren, nachvollziehbaren und effizienten Bewirtschaftung der eingesetzten Rollboxen verschiedene (teil-) automatisierte Lösungsvarianten evaluiert.

Es wurde eine Lösung mit passiven RFID-Tags und einer Lademittelverwaltungsapplikation, welche durch die Swiss Post Solutions / E-Business Solutions AG entwickelt wurde, zur Umsetzung ausgewählt.

Diese Fallstudie beschreibt die Ausgangslage des Projektes, die Projektstruktur sowie erste Erfahrungen aus dem produktiven Betrieb.

2 Grundlagen RFID

Obwohl RFID seit einigen Jahren viel Beachtung geschenkt wird, wurde die zugrunde liegende Idee bereits seit 1939 im Zweiten Weltkrieg zur Freund-Feind-Erkennung bei Flugzeugen benutzt.[1] Stockman hat 1948 in seinem Beitrag „Communication by means of reflected power“ die Technologie erstmals detailliert beschrieben.[2] Die fortschreitende Miniaturisierung führt zu einem immer breiter werdenden Anwendungsfeld. So wird darüber diskutiert, einzelne Transponder nicht nur auf Paletten oder Containern zu platzieren, sondern diese als Ersatz von Barcodes einzusetzen. Aufgrund der wesentlich grösseren Datenmenge, welche ein Transponder gegenüber einem Barcode aufweist, kann dieser nicht nur eine Produktgruppe, sondern die einzigartige Ausprägung des Produkts identifizieren.[3] Es wird davon ausgegangen, dass dieser Einsatz von RFID-Tags bei Produktion und Transport von Gütern lohnenswert wird, sobald der Preis pro Transponder die Grenze von 5 Euro Cents unterschreitet.[4]

2.1 Technologie

2.1.1 Architektur

Ein RFID-System besteht aus

- einem oder mehreren Tags (auch Transponder genannt)

- einem oder mehreren Empfängern

- sowie einem oder mehreren Backend-Systemen.[5]

Der idealtypische Aufbau eines RFID-Systems ist in Abbildung 1 zu sehen.

[1] Garfinkel, Juels et al., 2005, S. 34.
[2] Stockman, 1948.
[3] Weis, Sarma et al., 2003, S. 201 f.
[4] Juels, 2006, S. 381.
[5] Weis, Sarma et al., 2003, S. 203.

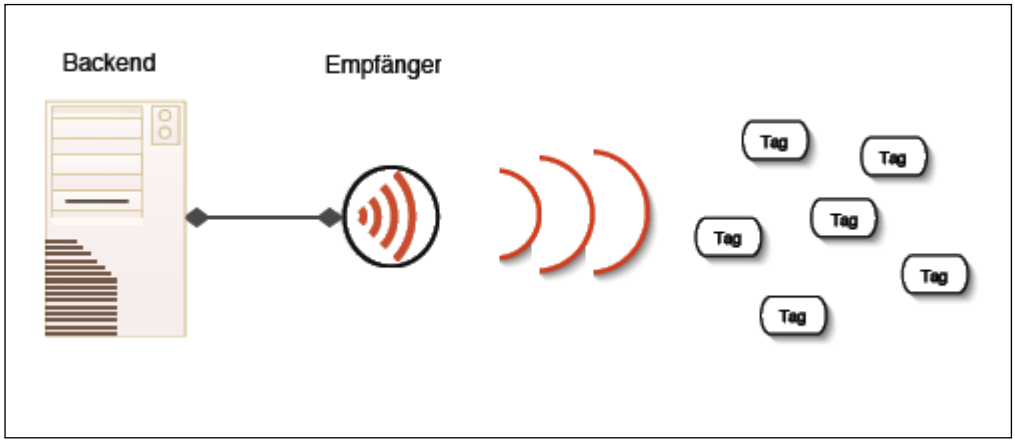


Abbildung 1: Aufbau eines RFID-Systems[6]

Obwohl im Allgemeinen davon ausgegangen werden kann, dass ein Empfänger mit mehreren Tags kommunizieren kann, ist es auch möglich, dass ein RFID-System lediglich aus einem Empfänger und einem Tag besteht. Beispiele für Tags sind in Abbildung 2 dargestellt.

Abbildung 2: Verschiedene Arten von RFID-Tags[7]

[6] Vgl. Avoine, 2005, S. 60.
[7] Coresonant, 2014.

Ein Tag muss in einem RFID-System nicht zwingend mit einer Batterie versehen sein, sondern kann seine für einfache Rechenoperationen benötigte Energie aus dem Radio- oder Magnetfeld des Lesegeräts beziehen. Die Bezeichnungen „Reader“ oder Empfänger sind irreführend, da diese Geräte Energie und Information ausstrahlen müssen, um Daten empfangen zu können.

2.1.2 Klassifikationsmerkmale von Tags

Im Folgenden werden Unterscheidungsmerkmale von Tags kurz erläutert.[8]

Energie

Die Energie, welche ein Tag benötigt, kann entweder von einer externen oder internen Quelle stammen. Aktive Tags besitzen eine eigene Batterie, welche zur Kommunikation und Datenverarbeitung genutzt werden kann. Halb-passive Tags sind zwar ebenfalls mit einer Batterie ausgestattet, diese dient aber nur zur Datenverarbeitung auf den Tags und nicht zur Kommunikation. Passive Tags beziehen die gesamte benötigte Energie über ein elektromagnetisches Feld vom Empfänger. Halb-passive und aktive Tags sind teurer als passive Tags und haben eine kürzere Lebensdauer.

Kommunikationsdistanz

Die maximale Kommunikationsdistanz der Tags hängt von mehreren Faktoren ab. So ist zum einen die benutzte Kommunikationsfrequenz entscheidend. Die maximale Distanz von Ultrahochfrequenztags (UHF) zum Empfänger kann mehrere Meter betragen, während diese bei Hochfrequenztags im Meterbereich liegt. Bei Niedrigfrequenztags sinkt sie auf den Zentimeterbereich. Weiter ist die Feldstärke des Empfängers entscheidend, welche durch diverse Standards weltweit beschränkt ist. Die Feldstärke eines Senders sinkt im Quadrat zur Distanz, deshalb ist die maximale

[8] Abschnitt 2.1.2 basiert auf Avoine, 2005, S. 62 ff.

Kommunikationsdistanz auch in Zukunft auf die genannten Distanzen physikalisch beschränkt.[9]

Die Lesedistanz der Tags kann, wenn von einem bösartigen Empfänger mit speziellen Antennen und/oder nicht gesetzeskonformen Sendestärken ausgegangen wird, erheblich von der nominellen Lesedistanz abweichen.

Speicher

Die Speicherkapazität der Tags kann ebenfalls zu ihrer Unterscheidung herangezogen werden. Während Diebstahlsicherungen lediglich ein Bit benötigen (Diebstahlsicherung aktiv/inaktiv), sind bei komplexeren Tags zwischen 32 und 128 Bits für ihre Identifikation reserviert. Der Tag kann, je nach benötigtem Einsatz, ROM, EEPROM, RAM oder SRAM Elemente besitzen.

Rechenkapazität

Die Rechenkapazität ist ein weiteres Unterscheidungsmerkmal der Tags. Einige sehr einfache Tags können lediglich ihre Identifikation senden und keinerlei Operationen ausführen. Die nächste Stufe von Tags kann einfache XOR und AND Befehle ausführen. Sie haben aber nicht genug Kapazität für komplexere kryptographische Rechenoperationen. Es existieren auch Tags, auf welchen asymmetrische Kryptographie[10] implementiert werden kann.

Die Abgrenzung zwischen einzelnen Stufen ist fliessend und schwierig zu klassifizieren. Beim Protokolldesign werden oft implizite oder explizite Annahmen betreffend der Rechenkapazität von Tags gemacht. Auf die

[9] Weis, 2003, S. 21.

[10] Bei asymmetrischer Kryptographie (auch Public-Key Kryptographie genannt) wird, im Gegensatz zur symmetrischen Kryptographie, nicht ein gemeinsamer geheimer Schlüssel zwischen Sender und Empfänger geteilt, sondern jeder Teilnehmer hat je ein Schlüsselpaar, bestehend aus privatem und öffentlichem Schlüssel. Die Nachricht wird vom Sender mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und kann ausschliesslich mit dem dazugehörigen privaten Schlüssel des Empfängers entschlüsselt werden. Aufgrund der oft komplexen Algorithmen werden höhere Ansprüche an die Rechenleistung als bei symmetrischen Verfahren gestellt. Bekannte Beispiele für asymmetrische Kryptographie sind z.B. pgp zum Verschlüsseln von Mail oder https. Cobb/LeFrançois, 2014, S. 243 ff.

Rechenkapazität der Tags muss bei der Auswahl und Implementation von RFID-Systemen geachtet werden.

Manipulationssicherheit

Die Anforderungen an die physische Widerstandsfähigkeit von Tags gegenüber Manipulationsversuchen sind ebenfalls ein wichtiges Unterscheidungskriterium. Einfache Tags, welche lediglich eine statische Identifikationsnummer aussenden, müssen keinerlei Ansprüche an die Widerstandsfähigkeit gegenüber Angriffen haben, da auch ein erfolgreicher Angriff zu keinerlei zusätzlichen Informationen führen würde. Demgegenüber sollten komplexere Tags, welche ein in mehreren Tags vorhandenes Geheimnis wie z.B. einen kryptographischen Schlüssel beinhalten, gegenüber physischen Attacken möglichst resistent sein. Ansonsten würde die Analyse eines einzelnen Tags die Sicherheit des gesamten Systems beeinträchtigen.

Physische Charakteristiken

Die Antenne eines RFID-Transponders benötigt mehr Platz als der eigentliche Chip. Die Grösse der Antenne hängt im Wesentlichen von der benutzten Frequenz und der gewünschten Kommunikationsdistanz ab. Es ist zu beachten, dass unter einem Transponder nicht nur Schaltkreis und Antenne verstanden wird, sondern die komplette Einheit aus Schaltkreis, Antenne sowie Träger-Etikett oder -Plattform (siehe Abbildung 2).

Kommunikationsfrequenz

Für RFID werden diverse Frequenzbereiche genutzt. Da wesentliche Eigenschaften (Kommunikationsdistanz, Datentransferrate, Störung durch Elemente usw.) durch die Frequenz bestimmt werden, ist die Wahl einer Frequenz in erster Linie vom gewünschten Einsatzgebiet abhängig. Vier Frequenzbereiche werden hauptsächlich für RFID benutzt: 125-134 kHz (LF), 13,553-13,567 MHz (HF), 860-960 MHz (UHF) sowie 2.4000-2.4835 GHz (UHF).

Die Tags mit 13,553-13,567 MHz (HF) und 860-960 MHz (UHF) sind aufgrund ihrer Eigenschaften betreffend Kommunikationsdistanz und Datentransferrate besonders für Applikationen im Supply Chain Management (SCM) geeignet.

Standards

Zu RFID-Transpondern bestehen im Wesentlichen zwei Standardisierungen:
1. International Standards Organisation (ISO) und

2. EPC-Global.

EPC-Global ist eine Non-Profit-Organisation, welche 2003 aus dem Auto-ID-Center hervorgegangen ist. EPC kennt vier Klassen von Tags.[11]

2009 waren lediglich Klasse 1 Tags standardisiert (Class 1 Gen 2). ISO hat die von EPC-Global standardisierten Spezifikationen in die ISO Standards als Standard ISO 18000-6:2010 (bzw. ISO/IEC 18000-6:2013) übernommen.[12]

Koppelung und Datenübertragung

Die Art des Energieempfangs ist ein weiteres Unterscheidungsmerkmal. Während Niedrig- und Hochfrequenztags mittels induktiver Koppelung mit magnetischen Feldern mit Energie versorgt werden, beziehen Hoch- und Ultrahochfrequenztransponder ihre Energie mittels elektromagnetischer Koppelung von Radiofeldern. Tabelle 1 fasst die Unterscheidungsmerkmale der Tags im Hinblick auf EPC-Klasse, Speicher, Stromquelle und Einsatzmöglichkeit zusammen.

[11] Flörkemeier, 2005, S. 92.
[12] ISO, 2010, ISO, 2013.

Standard EPC-Klasse	Speicher	Stromquelle	Einsatzmöglichkeit
0	1 BIT	Passiv	Diebstahlsicherung
1	Lese	Jede möglich	Identifikation
2	Lese/Schreib	Jede möglich	Track and Trace
3	Lese/Schreib	Halb-passiv/aktiv	Umweltsensoren
4	Lese/Schreib	Halb-passiv/aktiv	Ad-Hoc-Netzwerke

Tabelle 1: Klassifikationsmerkmale von Tags[13]

2.2 Markt

Der Markt für RFID-Tags war bereits zum Zeitpunkt der Projektevaluation etabliert. So wird RFID z.B. für Strassengebühren (wie Télépéage in Frankreich oder Telepass in Italien), Haustiermarkierung, Ski-Pässe, elektronische Fahrkarten (wie die Oyster Card in London) in der Logistik und für weitere Anwendungen verwendet.[14] Auch steht die „Etikettierung" von Kindern in Vergnügungsparks oder Spitälern zur Diskussion.[15] Das Spektrum von Anwendungen zeigt, dass RFID auf breiter Basis angewendet wurde.

2009 wurde RFID das grösste Wachstumspotenzial beim Lagermanagement und in Anwendungen der Supply Chain bescheinigt. Die bis anhin verwendeten Strichcodes könnten durch einfache und billige Tags ersetzt werden. Dies würde die effizientere Gestaltung diverser Prozesse, wie z.B. Warenannahme durch automatisierte Massenerfassung von Waren, ohne direkten Sichtkontakt ermöglichen.[16]

Bis anhin erfolgte eine RFID-Etikettierung einzelner Waren nur im Hochpreissegment. 2009 wurden vor allem Paletten oder Behälter mit Tags ausgestattet. Mit der Senkung der Kosten pro Transponder ist zu erwarten,

[13] Vgl. Weis, 2003, S. 19.
[14] Vgl. Garfinkel, Juels et al., 2005, S. 34 f.
[15] Vgl. etwa Adventim, 2010.
[16] Santos/Smith, 2008, S. 128.

dass in Zukunft die Markierung einzelner Produkte stark an Bedeutung gewinnen wird.[17]

Aus dem Auto-ID-Center gingen im Jahre 2003 EPC-Global sowie die Auto-ID-Labs hervor. EPC-Global wurde mit dem Ziel gegründet, die Nutzung von Low-Cost RFID-Tags als Barcodeersatz zu fördern und die Tags zu standardisieren, während die Auto-ID-Labs sich mit Forschungsaspekten des RFID-Einsatzes beschäftigen.[18]

EPC-Global hat für die Nutzung der RFID-Infrastruktur das EPC-Global-Network gegründet. Dieses basiert mit einem Object Name Service (ONS) auf einer Analogie zum Internet mit dem Domain Name Service (DNS). Im ONS ist für jede Objekt-Nummer eine IP-Adresse hinterlegt, welche dem Anfragenden genaue Auskunft über Herkunft des Objektes geben kann.[19] So kann in Zukunft die Lücke zwischen Informationssystemen und der physischen Welt geschlossen werden, da realen Objekten eindeutige und automatische Identifikationen in Datenbanken zugeordnet werden können. Eine ubiquitäre Anwendung von RFID, z.B. im Rahmen eines globalen EPC-Global-Network, wird auch „Das Internet der Dinge“ genannt.[20]

[17] Michael/McCathie, 2005, S. 627.
[18] Avoine, 2005, S. 65.
[19] Flörkemeier, 2005, S. 93.
[20] Z.B. Fleisch/Mattern, 2005; Atzori, Iera et al., 2010, S. 2787.

3 Unternehmensprofile

3.1 Die Post

Die Schweizerische Post wurde 1849 als Bundespost gegründet und beschäftigte als zweitgrösste Arbeitgeberin der Schweiz 2007 über 43'000 Personen. Sie bietet Dienstleistungen im Post-, Logistik- und Zahlungsverkehr an. Des Weiteren ist sie auch im öffentlichen Verkehr tätig.[21] Die Post bewältigt eine erhebliche Zahl von Warenbewegungen. An einem Arbeitstag fallen mehr als 15 Millionen Briefe und 400'000 Pakete an. Daraus ergibt sich auch eine organisatorische Komplexität, welche sich in 20'000 Fahrzeugen, 2'500 Poststellen, 3 Paketzentren sowie (ab 2009) 3 Briefzentren[22] niederschlägt.

Die Post war 2009 in sieben operative Geschäftsbereiche sowie elf Stabsstellen gegliedert, wie Abbildung 3 darstellt.

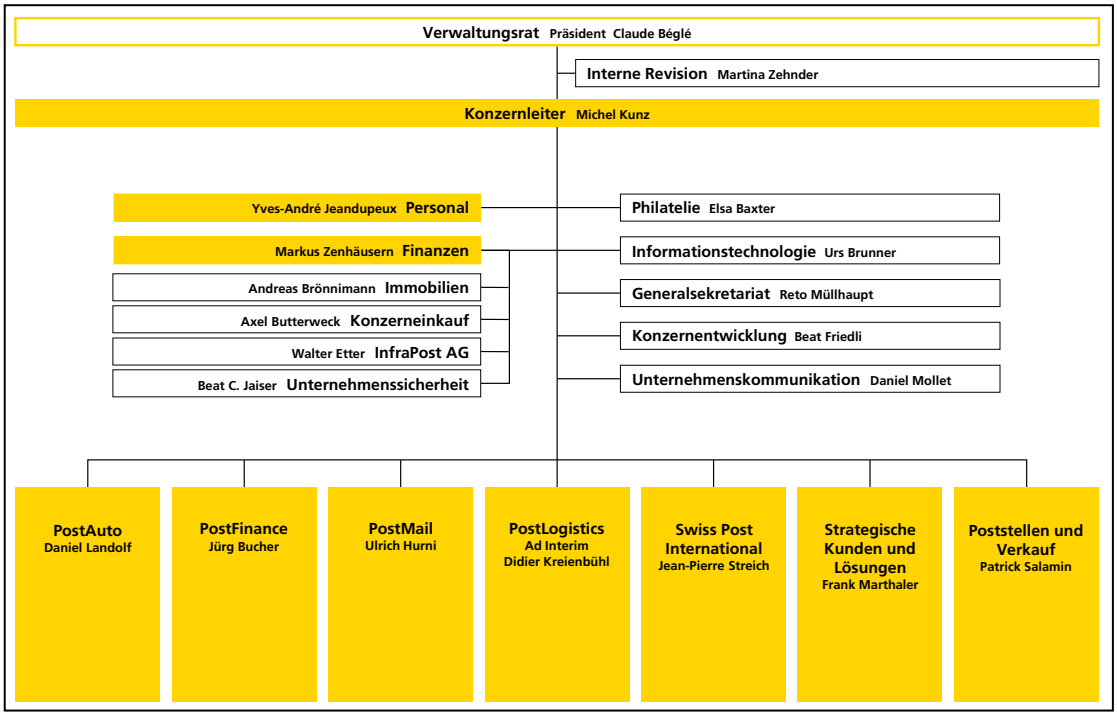


Abbildung 3: Organigramm der Post (2009)[23]

[21] Post, 2009b.
[22] Post, 2009a.
[23] Post, 2009c.

Am hier beschriebenen Projekt waren die Geschäftsbereiche PostLogistics (PL), Strategische Kunden und Lösungen (SKL) sowie die Stabsstelle Informationstechnologie (IT) beteiligt.

3.1.1 PostLogistics

PostLogistics (PL) ist als umfassender Logistikanbieter im Markt für Geschäfts- und Privatkunden positioniert.[24] Mit über 100 Millionen in der Schweiz zugestellten Paketen pro Jahr wird der Paketversand als Kerngeschäft von PostLogistics gesehen.[25]

3.1.2 Swiss Post Solutions AG

Aufgrund einer Bündelung der Geschäftstätigkeit wurden die Tochterfirmen der Post yellowworld AG, MailSource AG, DocumentServices AG, SwissSign AG, GHP Dialog Services GmbH und DCL Data Care AG im Konzernbereich SKL zusammengefasst.[26]

Die Swiss Post Solutions AG (SPS) ging zum 19.03.2008 aus der MailSource AG hervor, in welche die yellowworld AG sowie die DCL Data Care AG überführt wurden.[27] Der Bereich E-Business Solutions (EBS) der SPS trat am Markt vorerst weiterhin mit der Marke yellowworld als Co-Brand auf.

Die Applikation zur Lademittelverwaltung wurde durch Swiss Post Solutions AG entwickelt. Die Applikation basiert auf der „Integrated Platform E-Commerce“ (IPEC), auf welcher auf Kunden angepasste Prozesse in den Bereichen

- E-Billing,
- E-Commerce,
- E-Logistics und
- E-Archive

[24] PostLogistics, 2009b.
[25] PostLogistics, 2009a.
[26] Yellowworld, 2008.
[27] Handelsregister, 2008a; Handelsregister, 2008b.

entworfen und betrieben werden. So wurden im Jahr 2009 zwei Millionen Rechnungen und 500 Millionen Transaktionen sowie Umsätze der Kunden von 500 Millionen CHF abgewickelt. Der Aufbau der Plattform ist in Abbildung 4 dargestellt.

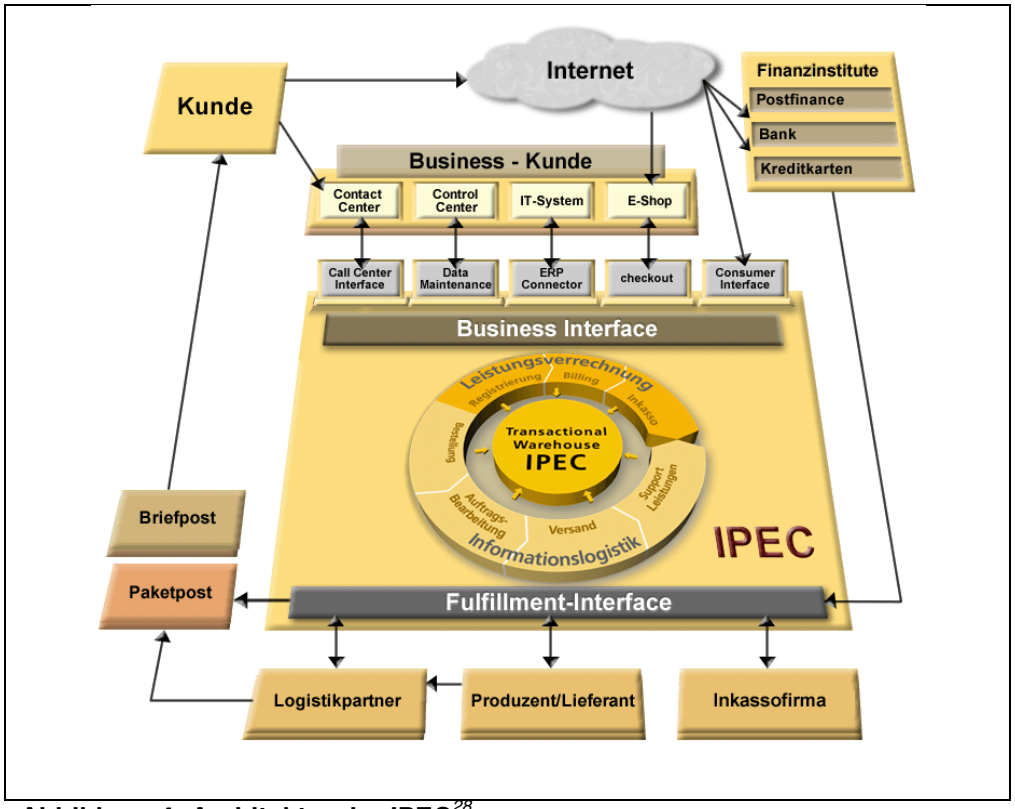


Abbildung 4: Architektur der IPEC[28]

3.2 Swisscom AG

Die Swisscom AG wurde per 1. Januar 1998 aus der Telekom/PTT gegründet. Der Börsengang erfolgte am 5. Oktober 1998.[29] Das Angebot der Swisscom umfasste 2009 für Auto-ID Technologien (und somit auch für das zugehörige Geschäftsfeld RFID) Consulting, Realisierung und Betrieb von Auto-ID-Lösungen (siehe **Abbildung 5**). Die Swisscom Auto-ID Services AG war organisatorisch dem Geschäftsbereich ”Strategie & Business Development Konzern“ zugeordnet.

[28] Yellowworld, 2006.
[29] Swisscom, 2008a.

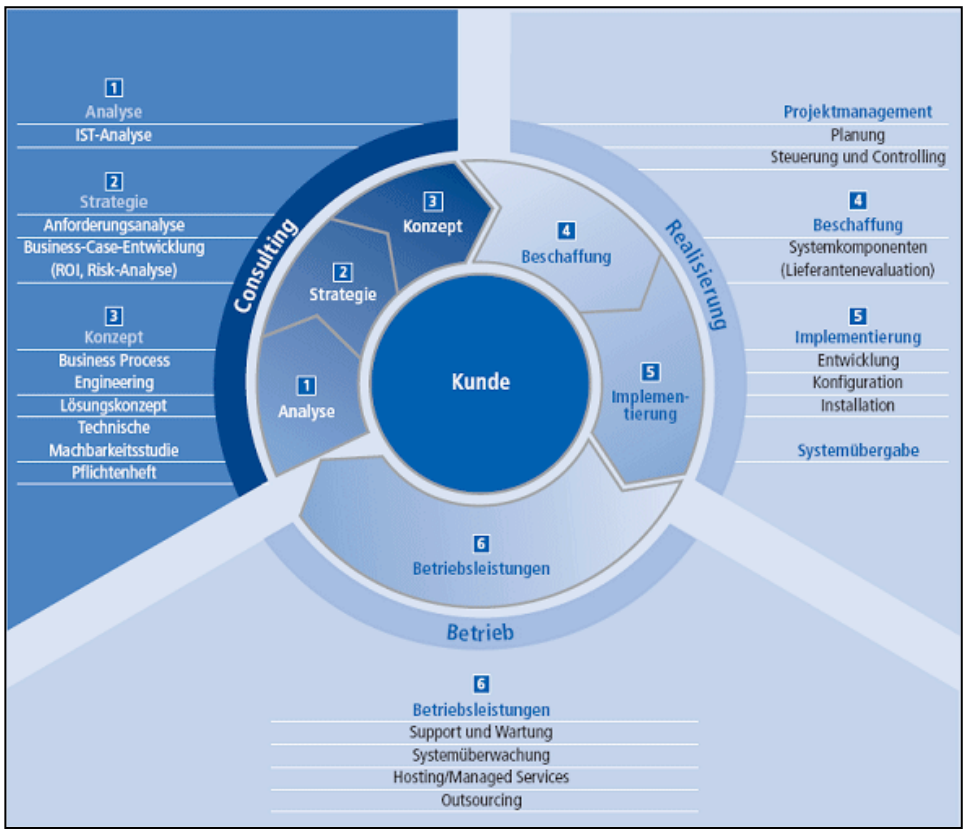


Abbildung 5: Marktangebot der Swisscom Auto-ID Services AG[30]

[30] Swisscom, 2006.

4 Lademittelverwaltung der Post

4.1 Problemstellung

Der Bewirtschaftung von Lademitteln wird durch Forschung und Praxis vermehrt Beachtung geschenkt.[31] Zum einen ist durch eine erhebliche Mittelbindung in Tauschgeräten ein effizientes Management angebracht. Ferner wirken sich, insbesondere bei der Post, Fehler und Unzulänglichkeiten in der Lademittelverwaltung direkt auf die operative Tätigkeit aus, wie z.B. durch verspätete Sendungen und Extra- oder Leerfahrten der Transportfahrzeuge.

Bei der Paketverteilung nutzt die Post drei Paketzentren, 31 Distributionsbasen, 20 Distributionsfilialen sowie 45'000 Rollboxen. Die geografische Verteilung der Standorte ist in Abbildung 6 dargestellt.

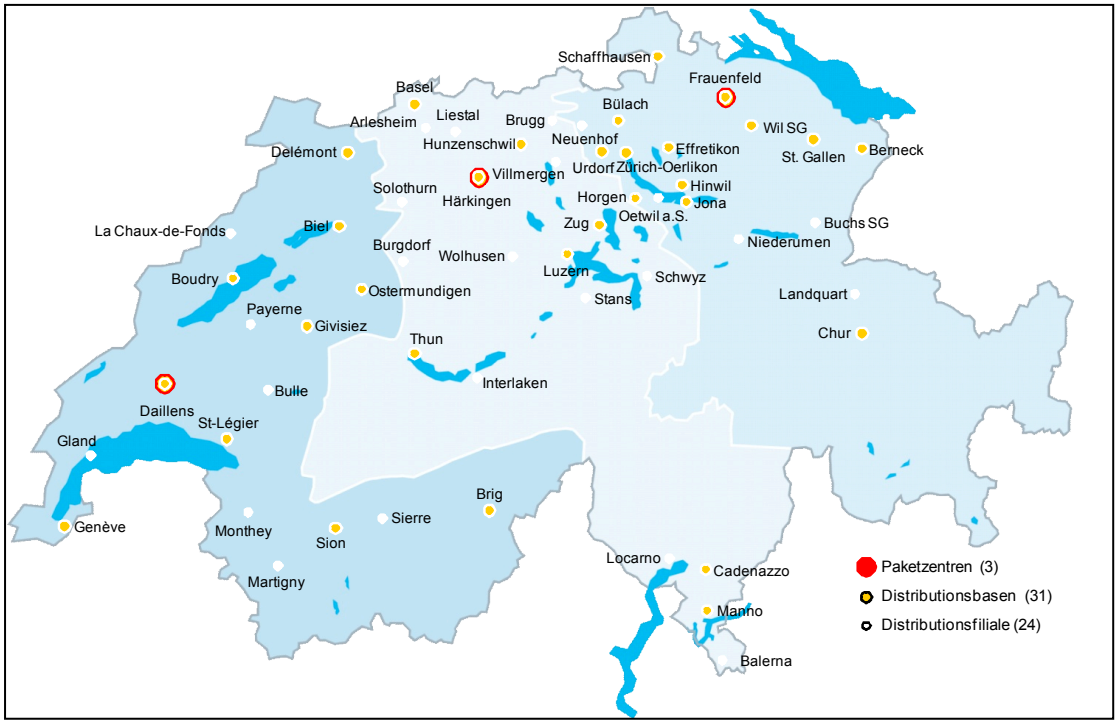


Abbildung 6: Standortübersicht für RX-Bewirtschaftung[32]

[31] Vgl. z.B. Dangelmaier, Pape et al., 2004; Kuhn, Lange et al., 2005; Knolmayer/Dedopoulos, 2006.
[32] Gafner, 2008b.

Einen Überblick über die durch PostLogistics im Jahr 2009 eingesetzten Rollboxen (RX) gibt Abbildung 7.

RX PP 2000	RX BP 2000	RX-2G	RX-Corlette
			
ca. 25'000 Stk.	ca. 6'000 Stk.	ca. 11'000 Stk.	ca. 3'000 Stk.

Abbildung 7: RX-Typen der PostLogistics[33]

4.2 Ist-Analyse

Die Bewirtschaftung von RX war für PL seit längerem ein Thema. Bereits im Jahr 1999 wurde in einem ersten Projekt die Bewirtschaftung der RX-Flotte der Post evaluiert. Es wurde beschlossen, zunächst eine Inventur der Rollboxen auf Basis einer Tabellenkalkulation aufzubauen, die technische Entwicklung (insbesondere von Transpondern und Barcode) aber weiter zu verfolgen. Im Jahr 2002 wurden Projektkosten und Einsparungen einer teilautomatisierten Lösung evaluiert. Ihre Realisierung für die gesamte Post wäre zu diesem Zeitpunkt aber nicht wirtschaftlich gewesen. Ein Pilotversuch mit Barcodescanning wurde 2003 in der Ostschweiz mit einem Paketzentrum, einer Distributionsbasis, 17 Poststellen sowie 10 Geschäftskunden durchgeführt. Dabei zeigte sich, dass ein schweizweiter Ausbau des Prototyps nicht ohne Weiteres möglich ist.

2005 hat eine SWOT(Strenght Weaknesses Opportunities Threats)-Analyse die Stärken und Schwächen sowie die Chancen und Gefahren der Ist-Situation in der RX-Bewirtschaftung aufgezeigt.[34] Als Stärken wurden die Prozesse, die Kontakte zu den Herstellern und das Transportnetz identifiziert.

[33] Gafner, 2008b.
[34] Vgl. zum Folgenden Borer/Schöni, 2005, S. 12.

Ferner wurden die Informationen über den Paketmengenfluss positiv beurteilt. Demgegenüber standen als Schwächen mangelnde Kenntnisse zu RX-Beständen, Nutzung und Standzeiten und damit einhergehend fehlende Möglichkeiten zur effektiven Planung der RX-Einsätze. Auch konnten die Fremdnutzung der RX und die Schadensursachen nicht eruiert werden.

Die Chancen einer erfolgreichen RX-Bewirtschaftung wurden in einem Abbau der Schwächen gesehen, d.h. es wurden Kostenersparnisse und eine verbesserte Leistungserbringung (z.B. Laufzeiten oder Personaleinsatz) erwartet.

Als Risiken wurden die Schnittstellen zu bestehenden Systemen, Investitions- und Betriebskosten und eventuell mangelnde Akzeptanz der Lösung ermittelt.

Beim Projektstart im Februar 2008 erfolgte eine Inventur der Rollboxen alle zwei Jahre, was die Planung, Steuerung und Bewirtschaftung der Rollboxen aufgrund des langen Inventurintervalls erheblich erschwerte. Trotz der aufwändigen manuellen Inventur waren keine exakten Bestandsdaten vorhanden und es trat ein erheblicher Schwund von Rollboxen auf.

4.3 Soll-Konzept

Für die RX-Bewirtschaftung wurden vier Muss- und drei Soll-Kriterien definiert, welche sich aus den Schwächen der manuellen Lösung ergeben. Eine Übersicht zu den Kriterien findet sich in Tabelle 2. Das Hauptziel des Projekts war, „dass genügend RX zur richtigen Zeit am richtigen Ort verfügbar sind.“[35]

[35] Borer/Schöni, 2005, S. 13.

Kriterium	Art des Kriteriums	Beschreibung
Mengenfluss	Muss	Durchgängige Anzeige der Mengenflüsse und Standzeiten
Beschaffung	Muss	Bestände sind exakt
Übergreifende Nutzung	Muss	Nutzung der RX durch andere Geschäftsbereiche oder Kunden sichtbar
Instandhaltung	Muss	Instandhaltungsplanung und -kontrolle
Fehlverlad	Soll	Unterbindung von Fehlverladen der RX
Auslastung RX	Soll	Messung der Füllgrade
Austausch mit Kunden	Soll	Aufenthaltsort und -dauer von RX ausserhalb der Post

Tabelle 2: Kriterien der RX-Bewirtschaftung

4.4 Evaluation und Entscheid

In der Voranalyse des Projekts wurden die Lösungsansätze und eingesetzten Technologien neun anderer Unternehmen mit einer komplexen Logistik als Vergleichsbasis ausgewertet. Daraufhin wurden folgende technischen Möglichkeiten zur RX-Datenerfassung miteinander verglichen:

- Variante 1: Taster an den Toren
- Variante 2: Barcode - manuelles Scanning
- Variante 3: Barcode - automatisches Scanning
- Variante 4: Presence RFID aktiv
- Variante 5: Presence Wireless RFID aktiv
- Variante 6: Gate RFID passiv
- Variante 7: GPS

Es folgt ein kurzer Überblick zu den einzelnen Varianten.

4.4.1 Variante 1: Taster an den Toren

Bei dieser Variante wären die Anzahl der ein- und ausgeladenen RX manuell über eine numerische Tastatur am Verladetor erfasst worden. Geringe Investitionen stünden hier einer durch den manuellen Prozess bedingten hohen Fehleranfälligkeit gegenüber.

4.4.2 Variante 2: Barcode - manuelles Scanning

Die an den RX angebrachten Barcodes wären durch den Mitarbeiter manuell gescannt worden. Diese Variante entsprach im Wesentlichen dem nicht erfolgreichen Pilotprojekt von 2003.

4.4.3 Variante 3: Barcode - automatisches Scanning

Die an den RX angebrachten Barcodes wären bei der Durchfahrt durch die Verladetore automatisch gescannt worden. Hier wurden hohe Investitionskosten erwartet, da sämtliche Tore mit mehreren optischen Lesesystemen ausgestattet werden müssten.

4.4.4 Variante 4: Presence RFID aktiv

Hier wären in allen Paketzentren flächendeckend RFID-Lesegeräte angebracht worden, welche die Position der mit aktiven Tags (d.h. Tags mit Batterie) ausgestatteten RX im Paketzentrum ermittelt hätten. Bei dieser Variante wären zum einen hohe Kosten pro RFID-Tag angefallen, ferner hätten die Tags aufgrund der Batterien eine begrenzte Lebensdauer gehabt.

4.4.5 Variante 5: Presence Wireless RFID aktiv

Bei dieser Variante hätten die Leser im Gegensatz zu Variante 4 nicht über Kabel, sondern kabellos (wireless) kommuniziert. Zu den Überlegungen der Variante 4 wären hier die Risiken einer gestörten Funkkommunikation hinzugekommen.

4.4.6 Variante 6: Gate RFID passiv

Die RX werden mit passiven RFID-Tags ausgestattet und bei jeder Tordurchfahrt gelesen. Während die Investition in die Leser höher als bei Varianten 4 und 5 ausfällt, sind die Kosten pro RX deutlich geringer.

4.4.7 Variante 7: GPS

Bei dieser Variante wären die RX mit Transpondern ausgestattet worden, die ihre Positionen via Satelliten des Global Positioning Systems (GPS) übermittelt hätten. Da ein Lesen in Gebäuden oder LKWs sehr fehleranfällig

wäre, hätten in den Gebäuden und LKWs Signalumsetzer eingebaut werden müssen, um die Daten der RX zuverlässig zu empfangen.

4.4.8 Gegenüberstellung der Varianten

Das Nutzenpotenzial ist für alle Varianten gleich hoch und besteht aus dem Wegfall der manuellen RX-Zählung, der Optimierung der Leertransporte sowie der Reduktion von Fremdnutzung und Instandhaltungskosten. Der erwartete Nutzen der verschiedenen Varianten ergibt sich aus der möglichen Ausschöpfung des Nutzenpotenzials.

Die Zahlenwerte wurden von der Post als vertraulich eingestuft, so dass hier lediglich Rangfolgen angegeben werden können. Die Werte der nachfolgenden Tabelle entsprechen daher dem Rang einer Variante im Vergleich zu den restlichen Varianten für diese Zeile, d.h. ein Wert von 1 entspricht dem ersten, ein Wert von 7 dem letzten Platz. Sowohl von Variante 6 als auch von Variante 7 wird eine hundertprozentige Ausschöpfung des Potenzials erwartet. Dem erwarteten Nutzen der Varianten stehen die Kosten gegenüber, welche in der Tabelle 3 ebenfalls nur über Rangfolgen dargestellt werden können.

	Variante 1	**Variante 2**	**Variante 3**	**Variante 4**	**Variante 5**	**Variante 6**	**Variante 7**
Nutzenpotenzial	1	1	1	1	1	1	1
Ausschöpfung Nutzenpotenzial	30%	60%	60%	70%	70%	100%	100%
Nutzen in 5 Jahren	7	5	5	3	3	1	1
Projektkosten	1	2	7	5	3	4	6
Betriebskosten für 5 Jahre	1	6	4	1	1	4	7
Total Kosten	1	5	6	3	2	4	7
Erfolg	3	5	6	4	2	1	7

Tabelle 3: Kosten und Nutzenvergleich

Bei Verwendung der vertraulich zu behandelnden Daten zeigt sich, dass Variante 6 die beste erwartete Rendite sowie die höchste Abdeckung der Kriterien aufweist. Des Weiteren ist sie im Hinblick auf künftige Ausbaumöglichkeiten am flexibelsten. Aus diesen Gründen wurde das Projekt mit passiven RFID-Tags durchgeführt.

5 Rollboxenbewirtschaftung mit RFID

5.1 Projektstruktur

Die Realisierung des Projekts wurde in drei sogenannte Lose aufgeteilt: Los 1 beinhaltet die RFID-Infrastruktur, Los 2 die Verwaltungsapplikation. Die Verwaltungsapplikation ist eine von SPS zum Management von Lademitteln entwickelte Software. Die unterstützende Infrastruktur wie z.B. Netzwerke wurden im dritten Los zusammengefasst. Während Los 1 und 2 per Einladungsverfahren ausgeschrieben wurden, lag Los 3 im Bereich der IT Post. Anbieter konnten sich auf ein oder beide ausgeschriebenen Lose bewerben. Ein Überblick zur Projektstruktur findet sich in Abbildung 8.

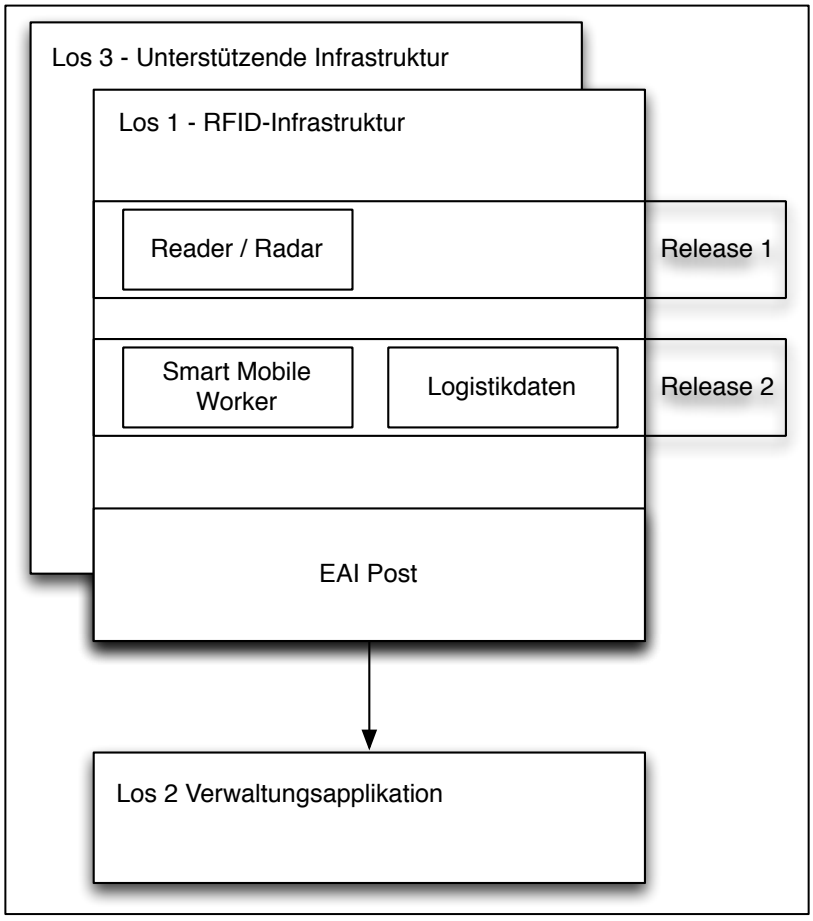


Abbildung 8: Projektstruktur RX-Bewirtschaftung

Das Projekt wurde in zwei Realisierungsphasen getrennt. Die flächendeckende Bereitstellung wurde als Release 1 bezeichnet. Auf dieser

Basis wurden im Laufe des Jahres 2009 mit Release 2 die Logistikdaten (Füllgrad und Destination) mittels mobiler Datenerfassung (Smart Mobile Worker) angebunden.

5.1.1 RFID-Infrastruktur und EAI (Los 1)

Den Zuschlag für die Aufgaben aus Los 1 hatte die Swisscom erhalten. Die Swisscom tritt gegenüber PL als Generalunternehmer auf und koordiniert den Einsatz von RFID-Hardware und Middleware. Ferner stellt sie die Kommunikation zwischen den Readern und den Backend Systemen sicher. Als Middleware zwischen den RFID-Lesern und der Enterprise Application Integration (EAI) der Post wird ein Edge Server der Seeburger AG verwendet. Die Seeburger AG ist auf Software für den intra- und interorganisationalen Datenaustausch und Prozessintegration spezialisiert.[36]

Die Kommunikation zwischen Los 1 und der Verwaltungsapplikation wird durch die Enterprise Application Integration (EAI) der Post sichergestellt. Die EAI Post stellt auf Basis von Web Services standardisierte Schnittstellen zu Umsystemen sicher.

In diesem Fall wird dem RFID-System durch die EAI ein Web Service angegeben, an welchen es die Ereignisse übergeben kann. Die EAI liefert die Daten asynchron an die IPEC-Plattform weiter und stellt den Empfang sicher. Ein schematischer Ablauf ist in Abbildung 9 dargestellt.

[36] Seeburger, 2009.

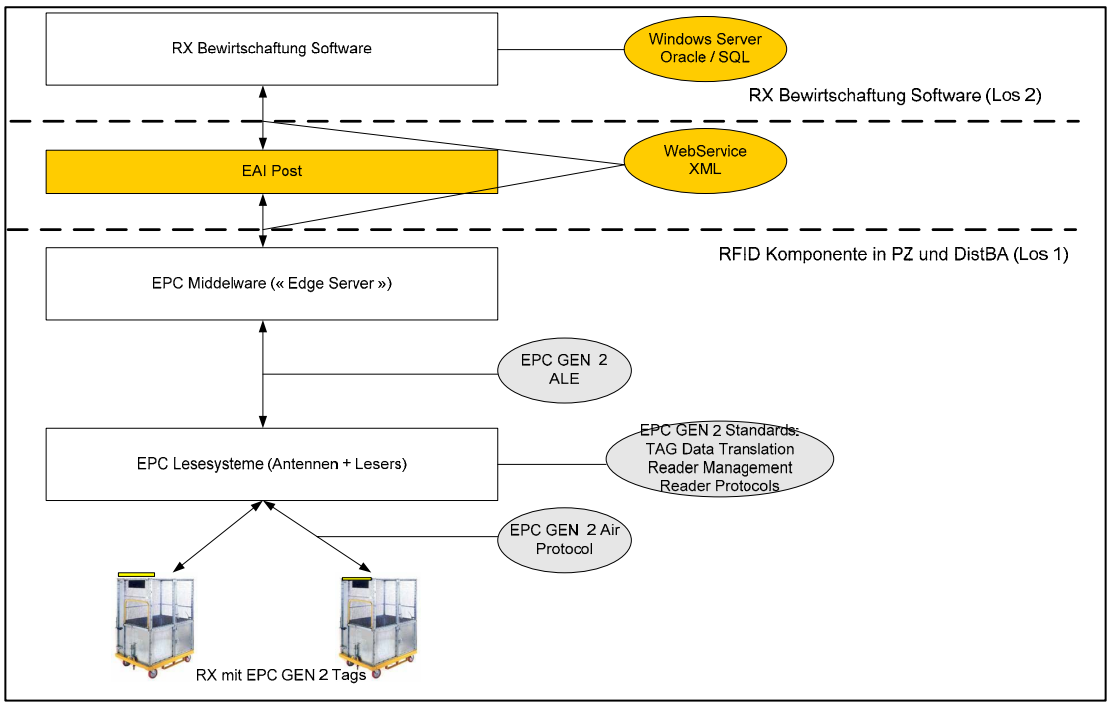


Abbildung 9: Datenübergabe mittels EAI[37]

5.1.2 Verwaltungsapplikation (Los 2)

Die Verwaltungsapplikation, welche durch SPS/EBS entwickelt und betrieben wird, löst anhand von verschiedenen Events (vgl. Tabelle 4) Geschäftsvorfälle aus. Als maximale Last an die Verwaltungsapplikation wurden 5'000 Buchungen pro Stunde und 100'000 Buchungen pro Tag definiert.

Event	Geschäftsvorfall
RX-Ausgang wird registriert	Buchung in Transit
RX-Eingang wird registriert	Buchung in Bestand des Standorts
Für eine RX wird 3 Tage keine Bewegung aufgezeichnet	Buchung an Extern

Tabelle 4: Events der Verwaltungsapplikation

Wie aus den Geschäftsvorfällen ersichtlich wird, handelt es sich um ein buchungsbasiertes System, wobei immer ein Konto und Gegenkonto bebucht werden. So wird beispielsweise bei der Ankunft einer RX in einem

[37] Gafner, 2008a.

Paketzentrum die RX aus dem Konto „in Transit“ abgebucht und auf das Bestandskonto des Paketzentrums eingebucht.

Anhand der immer aktuell vorhandenen Bestandes- und Flussinformationen können folgende Auswertungen in Echtzeit vorgenommen werden:

- Bestandes- und Transitkonten und administrative Ansichten
- Verfügbarkeit
- Bewegungen
- Standdaueranalyse
- Analyse der Flüsse
- Statistiken je Objekt
- Wartungsplanung
- Objekteinsatzdauer.

5.1.3 Unterstützende Infrastruktur (Los 3)

Die Aufgaben aus dem Los 3 wurden von der IT Post wahrgenommen. Es handelt sich hier in erster Linie um Netzwerke und die Verkabelung, welche an den Einsatzorten der Lesegeräte eine stabile Netzwerkverbindung zu den Edge Servern und von diesen zur EAI Post sicherstellen müssen.

5.2 Entwicklungspotenzial

Im Laufe des Jahres 2009 wurden die Rollboxen zusätzlich zum RFID-Tag mit Barcodes versehen, anhand welcher die Destination der RX sowie der Füllstand (leer, halbvoll, voll) durch den Mitarbeiter selektiert werden kann. An Standorten, welche mit RFID-Lesern ausgerüstet sind, erfolgt die Identifikation einer RX weiterhin mittels RFID. Ausschliesslich die Zusatzdaten (Destination und Füllstand) werden durch Mitarbeiter mittels des Barcodes ausgelesen. Der Füllstand der RX wird dabei über an der RX angebrachten Etiketten (leer, halbvoll, voll) gescannt. In der Verwaltungsapplikation werden so zusätzliche Auswertungen zur Auslastung der RX und zu den Flüssen der nicht mit RFID ausgestatteten Standorte möglich.

Aufgrund der vom Projekt unabhängig durchgeführten Beschaffung von 20'000 mobilen Endgeräten, welche lediglich Barcodes und keine RFID-Tags lesen können, wurde der Ausbau der RX-Bewirtschaftung (Release 2) nicht mit RFID durchgeführt. Diese mobilen Endgeräte werden nicht nur als Plattform für den „Smart Mobile Worker“ genutzt, sondern sind auch für neun weitere Anwendungen im Einsatz. Technisch gesehen hätte der weitere Ausbau des Projekts durchaus auch mit RFID vollzogen werden können, eine Beschaffung von neuen mobilen Endgeräten vor dem Ende der Lebensdauer der mobilen Barcodeleser ist aber im Jahr 2009 als unwirtschaftlich beurteilt worden.

6 Beurteilung der Rollboxenbewirtschaftung

6.1 Beurteilung des technischen Systems

Die Kapselung des technischen Systems in drei Lose und der Einsatz einer EAI haben sich aus Sicht der Post bewährt. Durch die Trennung mussten die Spezifikationen eine erheblich höhere Qualität aufweisen, als dies bei einem durch ein Team geführtes Projekt notwendig gewesen wäre. Dies sorgt für eine höhere Qualität bei der technischen Umsetzung.

Gewisse Probleme im produktiven Betrieb bei Los 1 wurden durch eine Lieferung fehlerhafter RFID-Tags verursacht. Diese konnten auch durch ausgiebiges Testen nicht antizipiert werden, da es sich nicht um einen Totalausfall der Tags, sondern um Dateninkonsistenzen handelte.

Die Verwaltungsapplikation des Loses 2 konnte die Anforderungen und Erwartungen erfüllen und es ergaben sich keine Probleme während des produktiven Betriebes. Durch die bereitgestellten Auswertungen konnten die in der SWOT-Analyse identifizierten Schwächen abgedeckt und die Basis für eine effektive RX-Bewirtschaftung gelegt werden.

6.2 Risikobeurteilung

Für eine Risikobeurteilung des RFID-Einsatzes des Projekts müssen nicht alleine die RFID-Komponenten, sondern auch die Infrastruktur und Ersatzszenarien betrachtet werden.

6.2.1 Risiko der RFID-Komponenten und der Infrastruktur

Die eingesetzte Infrastruktur (Leseportale) wird nicht gesondert gegen Angriffe geschützt, da sich diese in nicht öffentlichen Bereichen des Firmengeländes befindet. Dies reduziert das Risiko von Angriffen durch Aussenstehende, während Angriffe durch Personal möglich bleiben.

6.2.2 Wert der RFID-Informationen

Das System wird von der Post als nicht geschäftskritisch gesehen, da selbst ein Totalausfall des Systems keine nennenswerten operativen Konsequenzen nach sich ziehen würde. Falls die RFID jedoch bis auf die Ebene des einzelnen Pakets weitergeführt wird, so können sich, je nach Ausgestaltung, operative Risiken ergeben.

Der Wert der individuellen Informationen einzelner RX ist wesentlich geringer als der Wert der aggregierten RX-Flussdaten in der Verwaltungsapplikation. So können aus den aggregierten Daten Informationen über Umschlagshäufigkeit, Fahrtwege und Standorte gewonnen werden. Der Zugriff auf die Verwaltungsapplikation sollte daher nur einem beschränkten Personenkreis zur Verfügung stehen. Insbesondere bei vergleichbaren Projekten im Verteidigungsbereich sollte der Absicherung des Backendsystems besonders Rechnung getragen werden.

Die Anfälligkeit des Systems auf die von Rihs[38] analysierten Angriffe wird als gering gesehen. Die Informationen der RX-Bewegungen sind an sich nicht von grosser Relevanz. Durch die grosse geografische Ausbreitung muss ein Angreifer für ein Abfangen der Daten erhebliche Mittel für ein lokalisiertes Abfragen der RFID-Kommunikation aufwenden, ohne Mehrwert gegenüber einer rein optischen Beobachtung zu erzielen.

6.2.3 Ersatzszenarien

Für den Fall eines RFID-Ausfalls existiert eine Ausweichmöglichkeit. So ist eine Datenerfassung ebenfalls über das Auslesen der an den RX angebrachten Barcodes möglich. Dies führt zwar aufgrund der manuellen Intervention zu Mehraufwand, wäre aber als Überbrückungslösung denkbar. Des Weiteren könnte bei kurzen Ausfallzeiten komplett auf eine Datenerfassung verzichtet werden.

[38] Rihs, 2009.

6.2.4 Fazit

Durch die vorhandene Ausweichlösung der Barcodes kann auch bei einem Totalausfall aller RFID-Komponenten die Verwaltungsapplikation weiter betrieben werden.

Insgesamt ist das Risiko des RFID-Einsatzes im betrachteten Anwendungsfeld als gering einzustufen. Eine Erweiterung der Anwendung auf das Tagging von einzelnen Paketen würde aber eine erneute Analyse der Risiken notwendig machen.

6.3 Marktpotenzial

Der Fokus der Weiterentwicklung der Applikation wird auf der Vereinfachung und Sicherung von RFID-gestütztem Datentausch zwischen Unternehmen liegen, sofern von einer weitergehenden Marktdurchdringung von RFID ausgegangen wird. Hier liegt sowohl ein grosses Marktpotenzial als auch ein beträchtliches Risiko für die beteiligten Unternehmen.

7 Fazit

Das beim Projektstart als grösstes RFID-Projekt[39] der Schweiz geplante Projekt der RFID-gestützten Lademittelbewirtschaftung wurde Mitte 2009 als Erfolg bewertet. Die Verwaltungsapplikation erfüllt die Erwartungen und läuft im produktiven Betrieb fehlerfrei und zuverlässig. Die in der SWOT-Analyse identifizierten Chancen konnten mit der effektiven Bewirtschaftung der RX wahrgenommen werden, wohingegen die Risiken wie die Systemintegration und Akzeptanz der Lösung kontrolliert werden konnten.

Eine Determinante des Erfolges war die Aufteilung des Gesamtprojekts in Lose, durch welche die Komplexität des Gesamtprojekts auf beherrschbare Niveaus heruntergebrochen werden konnte. Voraussetzung hierfür waren die detaillierten Spezifikationen, welche eine reibungslose Zusammenarbeit zwischen den Auftragnehmern der drei Lose ermöglicht haben.

Da aufgrund der Projektinitiatoren das Projekt als IT-Projekt geführt und die Projektleitung durch die IT wahrgenommen wurde, kam es trotz der technischen Komplexität zu keinen nennenswerten Beeinträchtigungen im produktiven Betrieb. Dazu beigetragen haben ausführliche Tests, so dass Probleme bereits vor dem Produktivstart erkannt und behoben wurden.

Abschliessend lässt sich sagen, dass der Einsatz von RFID zur Verbesserung des Lademittelmanagements zweckmässig und die Verwaltungsapplikation für dieses Einsatzszenario geeignet ist.

[39] Swisscom, 2008b.

Abkürzungsverzeichnis

DNS	Domain Name Service
EBS	E-Business Solutions
EEPROM	Electrically Erasable Programmable Read Only Memory
EPC	Electronic Product Code
HF	High Frequency
ID	Identifikation
IPEC	Integrated Platform E-Commerce
ISO	International Organization for Standardization
IT	Informationstechnologie
LF	Low Frequency
ONS	Object Name Service
PL	PostLogistics
PP	Paket Post
RAM	Random Access Memory
RFID	Radio Frequency Identification
ROM	Read Only Memory
RX	RollboXen
SCM	Supply Chain Management
SKL	Strategische Kunden und Lösungen
SPS	Swiss Post Solutions
SPS/EBS	Swiss Post Solutions / E-Business Solutions
SRAM	Static Random Access Memory
SWOT	Strenght Weaknesses Opportunities Threats
UHF	Ultra High Frequency
XOR	eXclusive OR (entweder oder)

Literaturverzeichnis

Adventim (2010). "RFID Wristbands - Amusement park." Abgerufen am 2015-01-30, von http://www.wristband-rfid.com/en/amusement_parks.html.

Atzori, L., Iera, A. und Morabito, G. (2010). "The internet of things: A survey." Computer networks 54(15): 2787-2805.

Avoine, G. (2005). "Cryptography in Radio Frequency Identification and Fair Exchange Protocols." École polytechnique fédérale de Lausanne. Abgerufen am 2015-01-19, von http://sites.uclouvain.be/security/download/papers/Avoine-2005-thesis.pdf.

Borer, M. und Schöni, E. (2005). "Voranalyse Rx-Bewirtschaftung." Interner Bericht, Post.

Cobb, S. und LeFrançois, C. (2014). “Encryption”, in: Computer Security Handbook. Hrsg: Bosworth, S., Kabay, M. E. und Whyne, E. Hoboken, John Wiley & Sons: 223-272.

Coresonant. (2014). "RFID Tags for Solar Module." Abgerufen am 2015-02-28, von http://www.coresonant.com/html/rfid-tags-for-solar-module-india.html.

Dangelmaier, W., Pape, U. und Rüther, M. (2004). "Steuerungssystem für Transportbehälter." IS-Report 2: 48-49.

Fleisch, E. und Mattern, F. (Hrsg), (2005). "Das Internet der Dinge." Berlin, Springer.

Flörkemeier, C. (2005). "EPC-Technologie - vom Auto-ID Center zu EPCglobal", in: Das Internet der Dinge. Hrsg: Fleisch, E. und Mattern, F. Berlin, Springer: 87-100.

Gafner, T. (2008a). "Rollboxen mit RFID bewirtschaften." Abgerufen am 2015-01-19, von http://www.asut.ch/files/pdf488.pdf?4263.

Gafner, T. (2008b). "Rx-Bewirtschaftung mit RFID Technologie." Abgerufen am 2015-01-19, von https://www.yumpu.com/de/document/view/29491313/gestion-des-rx-tcbe/11.

Garfinkel, S., Juels, A. und Pappu, R. (2005). "RFID Privacy: An Overview of Problems and Proposed Solutions." IEEE Security and Privacy, 3(3): 34-43.

Handelsregister (2008a). "Meldungs Nr 4486558." Abgerufen am 2009-01-10, von https://www.shab.ch/shabforms/servlet/web/PdfView?DOCID=4486558.

Handelsregister (2008b). "Meldungs Nr 4486688." Abgerufen am 2009-01-10, von https://www.shab.ch/shabforms/servlet/web/PdfView?DOCID=4486688.

ISO (2010). "ISO/IEC 18000-6:2010." Abgerufen am 2015-01-30, von http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=46149.

ISO (2013). "ISO/IEC 18000-6:2013." Abgerufen am 2015-01-30, von http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=59644.

Juels, A. (2006). "RFID security and privacy: A research survey." IEEE Journal on Selected Areas in Communications, 24(2): 381-394.
Knolmayer, G., Dedopoulos, I. (2006). “Neugestaltung des Lademittel Managements der Migros auf Basis von ASP.” Band 13 der ausgewählten Fallstudien der Akademischen Partnerschaft ECR Deutschland, Köln. Abgerufen am 2009-02-17, von http://www.ecracademics.de/neugestaltung_des_ lademittel-managements_der.php.
Kuhn, E., Lange, V. und Zimmermann, P. (2005). "Paletten-Management, Leitfaden für die Praxis." München, Vogel.
Michael, K. und McCathie, L. (2005). "The Pros and Cons of RFID in Supply Chain Management." International Conference on Mobile Business (ICMB’05): 623-629.
Post (2009a). "Die Post - Fakten und Zahlen." Abgerufen am 2009-02-10, von http://www.post.ch/de/index/uk-schweizerische-post/uk-dossiers/uk-dossier-fakten-zahlen.htm.
Post (2009b). "Die Post - Über uns." Abgerufen am 2009-02-17, von http://www.post.ch/de/index/uk-schweizerische-post.htm.
Post (2009c). "Organigramm." Abgerufen am 2009-02-20, von http://www.post.ch/de/uk-organigramm-der-post.pdf.
PostLogistics. (2009a). "PostLogistics - Pakete." Abgerufen am 2009-02-10, von http://www.postlogistics.ch/de/index_log/log_log_gk/log-pakete-gk.htm.
PostLogistics. (2009b). "PostLogistics - Über uns." Abgerufen am 2009-02-10, von http://www.postlogistics.ch/de/index_log/log-log-ueberuns.htm.
Rihs, S. (2009). "RFID Security Risks in Supply Chains: More than Privacy." International Journal of Enterprise Network Management 3(4): 347-357.
Santos, B. L. D. und Smith, L. S. (2008). "RFID in the Supply Chain: Panacea or Pandora's Box?" Communications of the ACM 51(10): 127-131.
Seeburger. (2009). "Geschichte." Abgerufen am 2015-01-30, von http://www.seeburger.de/unternehmen.html.
Stockman, H. (1948). "Communication by Means of Reflected Power." Proceedings of the IRE 36(10): 1196-1204. Abgerufen am 2015-01-30, von http://ieeexplore.ieee.org/iel5/10933/35777/01697527.pdf?tp=&isnumber=&arnumber=1697527.
Swisscom (2006). "Marktangebot Auto-ID Services." Abgerufen am 2009-02-10, von http://www.swisscom.com/AutoID/content/Market_Offer/.
Swisscom (2008a). "Geschichte." Abgerufen am 2009-02-10, von http://www.swisscom.com/GHQ/content/Portraet/Geschichte/.
Swisscom (2008b). "Swisscom und Post realisieren das grösste RFID-Projekt der Schweiz." Abgerufen am 2015-02-27, von https://www.swisscom.ch/de/about/medien/press-releases/2008/04/20080428_01_RFID.html.
Weis, S. (2003). "Security and privacy in radio-frequency identification devices." Massachusetts Institute of Technology (MIT). Abgerufen am 2015-01-30, von http://groups.csail.mit.edu/cis/theses/weis-masters.pdf.

Weis, S., Sarma, S., Rivest, R. und Engels, D. (2003). "Security and privacy aspects of low-cost radio frequency identification systems." Lecture Notes in Computer Science. Berlin, Springer. 2802**:** 454–469.
Wessel, R. (2007). "RFID kanban system pays off for Bosch." Abgerufen am 2015-01-30, von http://www.rfidjournal.com/article/view/3293.
Yellowworld (2006). "Informatikplattform – IPEC." Abgerufen am 2009-01-10, von http://www.yellowworld.ch/site/3329/default.aspx.
Yellowworld (2008). "Fusion in die Swiss Post Solutions AG." Abgerufen am 2009-01-10, von http://www.yellowworld.ch/aktuell/news/Umfirmierung-in-Swiss-Post-Solutions-AG.aspx.

5 Discovering Suppliers' Customers by means of Statistical Disclosure Attacks

For copyright reasons (no reprints) the original paper is not included. The full reference including the URL follows.

Rihs S. and Miede, A. (2014). Discovering Suppliers' Customers by means of Statistical Disclosure Attacks. *International Journal of RFID Security and Cryptography.* 3(1), pp. 148 – 155. http://infonomics-society.ie/wp-content/uploads/ijrfidsc/published-papers/volume-3-2014/Discovering-Suppliers-Customers-by-means-of-Statistical-Disclosure-Attacks.pdf .

6 Summary and Outlook

6.1 Summary

In the three papers presented in Sections 3, 4, and 5, aspects of RFID security in supply chains were analyzed from theoretical, empirical, and practical points of view. The results have implications for practitioners implementing RFID systems, as well as researchers analyzing the security of RFID.

The underlying research questions were:

- If and how does the use of RFID change the risk profile for a supply chain?
- What is the security impact of RFID in the use case of package item management?
- Assuming an increased attack surface stemming from RFID use in a distribution center, could traffic analysis be a potentially successful avenue of attack?

To answer the first question, a generic risk matrix concerning the use of RFID was designed and analyzed (Section 3). Closed- and open-loop RFID supply chains were analyzed with regard to the impact of different attacks. Eavesdropping and tag injection were shown to be the attacks having the highest impact and likelihood in supply chain environments with shared tags amongst partners. Furthermore, possible preventive and mitigating countermeasures were outlined, with a special recommendation for strengthening physical security measures in sensitive areas.

The second question was treated by analyzing a very large-scale RFID deployment for the management of package items at the Swiss Post (Section 4). A suitability analysis was conducted for the developed software and RFID, as well as a risk analysis for the RFID data and system. In conclusion, both the use of RFID and the developed software were found to be suitable for this application scenario. The risk of using RFID is low in this case, as there

is a complete fallback scenario (barcodes), and the information on the individual tags is less valuable than the aggregated information in the backend system.

The third research question was answered with a simulation model and the simulation of the vulnerability of an RFID-equipped supply chain distribution center to the statistical disclosure attack (SDA) (Section 5). The analysis showed that the success probability for the SDA varies depending on the number of customers and their structure, as well as on the organization of the distribution center. If there are multiple product deliveries to a customer per round, or if only a fraction of all deliveries are observed by the attacker, the success probability of the SDA decreases. If the fraction of observed rounds falls below a determined and calculable threshold, the attack is very improbable to succeed. This leads to possible countermeasures, such as padding shipments with extra tags and strengthening physical security measures that render observation and eavesdropping more difficult.

6.2 Outlook

With NFC on smartphones being a current driver of consumer demand, the usage of RFID and other ubiquitous technologies will likely continue to rise within the foreseeable future. Furthermore, in industry, the ongoing standardization of software and hardware is serving to lower the boundaries for the implementation of RFID in supply chains.

The increased use will make RFID systems more attractive targets for attackers, and will thus most likely result in more attacks. The addition of new functionalities in existing systems or the integration of additional systems in RFID projects could also lead to higher risk exposure in previously low-risk situations. For instance, the integration of a customer relationship system with an RFID shipping system could mean that additional data is linked to an RFID tag.

Switching from palette tagging to item-level tagging multiplies possibilities for attacks, both in terms of scope and impact. However, as seen in Section 5,

while item-level tagging increases possibilities for eavesdropping, it does not necessarily simplify the traffic analysis necessary for disclosure attacks if the number of shipments does not increase.

Further research is thus needed regarding both real life attacks on existing supply chain operations, as well as theoretical attacks and attack frameworks for the use of RFID in supply chains. A forensic analysis of a successful attack on an existing productive RFID system would lead to valuable knowledge about exploited vulnerabilities and could help in the design of better countermeasures. Implementing and publishing proof-of-concept attacks could also increase risk awareness regarding possible vulnerabilities of RFID in supply chains. In addition, further research regarding communication protocols for RFID systems and the subsequent analysis of their vulnerabilities should continue, as this will lead to more secure RFID systems.

All three of the presented papers show that special attention should be given to security aspects within supply chains when implementing new RFID projects or enhancing existing deployments with new functionalities.

6.3 Concluding Remarks

This thesis has spanned over a period of time in which the RFID market matured considerably. During interviews conducted with experts at the beginning of the thesis project, the majority of interviewees were preoccupied with technical implementation problems, such as antenna design and the possibility of cost savings. Another aspect of markets in early stages is the quick rise and disappearance of companies.[88]

With the emergence of standardized RFID equipment, such as printers and software solutions integrated into enterprise resource planning systems, the

[88] Three separate cooperation projects planned for this thesis have not come to fruition due to disappearance or economic problems of the companies, which has had a significant impact on the planning, design, and writing of this thesis.

focus of implementation has shifted towards efficiency gains, whereas security concerns have yet to emerge as a primary concern in implementation.

Last but not least, in addition to its academic contributions, this thesis should help to raise awareness of RFID-related supply chain security risks amongst practitioners. This should lead to the implementation of more secure RFID systems, which in turn will help to improve overall information system security.

Appendix A – Mathematical Development

Due to page constraints, the development of the formula for the required number of observations was excluded in the paper submitted on SDA (Section 5).

The development is shown below:

$$\mu_{Alice} - l\sigma_{Alice} > l\sigma_{Noise}$$

$$\frac{1}{m}t - l\left(\sqrt{\frac{m-1}{m^2}t}\right) > l\left(\sqrt{\frac{N-1}{N^2}(b-1)t}\right)$$

$$\frac{1}{m}t > l\left(\sqrt{\frac{m-1}{m^2}t}\right) + l\left(\sqrt{\frac{N-1}{N^2}(b-1)t}\right)$$

$$t > ml\left(\sqrt{\frac{m-1}{m^2}t}\right) + ml\left(\sqrt{\frac{N-1}{N^2}(b-1)t}\right)$$

$$t^2 > \left[ml\left(\sqrt{\frac{m-1}{m^2}t}\right) + ml\left(\sqrt{\frac{N-1}{N^2}(b-1)t}\right)\right]^2$$

$$t^2 > \left[ml\sqrt{t}\left(\sqrt{\frac{m-1}{m^2}} + \sqrt{\frac{N-1}{N^2}(b-1)}\right)\right]^2$$

$$t^2 > \left(\sqrt{t}\right)^2\left[ml\left(\sqrt{\frac{m-1}{m^2}} + \sqrt{\frac{N-1}{N^2}(b-1)}\right)\right]^2$$

$$t^2 > t\left[ml\left(\sqrt{\frac{m-1}{m^2}} + \sqrt{\frac{N-1}{N^2}(b-1)}\right)\right]^2$$

$$t > \left[ml\left(\sqrt{\frac{m-1}{m^2}} + \sqrt{\frac{N-1}{N^2}(b-1)}\right)\right]^2$$

Appendix B – Source Code

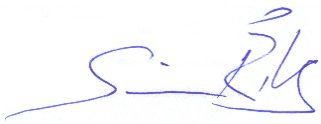
For copyright reasons, the source code of the Simulation model is not included.

The simulation was implemented using the Repast Simphony Framework, Version 2.1, and is JAVA-based. Unless otherwise noted, the code was provided by André Miede, Multimedia Communications Lab (KOM), TU Darmstadt, Rundeturmstraße 10, D 64283 Darmstadt, Germany (all rights reserved). Code developed by Simon Rihs is commented with the tag //SDR.

Statement of autonomous and independent work

„Ich erkläre hiermit, dass ich diese Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen benutzt habe. Alle Stellen, die wörtlich oder sinngemäss aus Quellen entnommen wurden, habe ich als solche gekennzeichnet. Ich erkläre mich einverstanden, dass diese Arbeit mittels Software auf Plagiate geprüft wird. Mir ist bekannt, dass andernfalls der Senat gemäss Artikel 36 Absatz 1 Buchstabe o des Gesetzes vom 5. September 1996 über die Universität zum Entzug des aufgrund dieser Arbeit verliehenen Titels berechtigt ist.“

„I hereby declare that I have written this thesis without any help from others and without the use of documents and aids other than those stated above. I have mentioned all used sources and cited them correctly according to established academic citation rules. I hereby agree that my thesis will be checked for plagiarism by detecting software. I am aware that otherwise the Senat is entitled to revoke the degree awarded on the basis of this thesis, according to article 36 paragraph 1 letter o of the University Act from 5 September 1996.“



Bern, 2015-06-15 Simon Rihs