We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

4,800
Open access books available

122,000
International authors and editors

135M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

CLARIVATE ANALYTICS BOOK CITATION INDEX INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

23

RFID System Architecture Reconsidered

Dirk Henrici, Aneta Kabzeva and Paul Müller
University of Kaiserslautern
Germany

1. Introduction

The RFID technology is already of high commercial relevance. It breaks into new application areas, and new markets are emerging. RFID becomes more and more an indispensable part of our everyday life. However, the technology also introduces security and privacy problems. Despite of the numerous research efforts, no satisfactory solutions for these issues have yet been found and widely implemented. For this reason, there are many people who take fright at RFID.

Today's RFID system architecture is carried over from the architecture used in other auto-id systems, chiefly optical barcode systems. As RFID introduces new functionalities and privacy risks, this classic architecture is no longer appropriate. For instance, the classic architecture fails to provide location privacy and self-determination for the affected users while being scalable and open. In this chapter, the problem is explained, the limitations in extending the classic architecture are outlined, and important aspects of a new architecture are sketched.

In the remainder of this first subchapter, an overview of the security and privacy goals and the main concepts for reaching them is provided. The requirements that RFID systems should fulfill are outlined in a separate section. The second subchapter introduces into the current RFID system architecture and the general direction of RFID security and privacy research. Subchapter 3 shows the practical deficiencies of the current architecture and illustrates, using an example, why incremental improvements and extensions lack to provide satisfactory solutions. Finally, considerations on how a completely new RFID architecture might look like are performed.

1.1 Security and privacy goals

There are five high-level issues of great importance for the RFID system security and the users' privacy [Henrici, D. (2008)]. Fig. 1 shows an overview on them. The remainder of this section provides a more detailed explanation of each goal.

Maintain data security: In many cases, RFID systems operate with privacy sensitive data that shall not become public. Such data may be some product information or even personal information. Security mechanisms for the prevention of illegal access to such data are one of the main challenges for RFID systems.

Prevent counterfeiting: With the change-over from barcodes to RFID, a better prevention of product counterfeiting is desired. Plagiarism in not only an economic issue but, e.g. in the case of drugs, can also be a mortal danger.

Source: Development and Implementation of RFID Technology, Book edited by: Cristina TURCU,
ISBN 978-3-902613-54-7, pp. 554, February 2009, I-Tech, Vienna, Austria

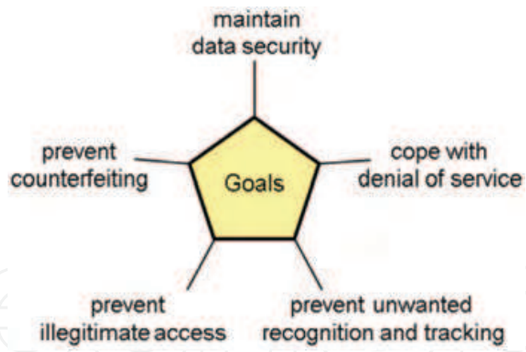

Fig. 1. Security and privacy goals for RFID systems [Henrici, D. (2008)]

Prevent illegitimate access: Reading an RFID tag, a reader creates a "read event" that is processed in the backend systems. It should be ensured that valid events cannot be generated by spoofed devices. This prevents, for example, that an attacker can fabricate events indicating a false location of an RFID tag. In general, illegitimate access to system components shall be effectively prevented.

Cope with denial of service: It is easy to put parts of an RFID system out of order. The reading of many kinds of RFID tags can be interfered with tinfoil, for example. Since a prevention of all denial of service attacks is not feasible, RFID systems should at least provide means for detection and recovery. RFID protocols should not introduce additional denial of service vulnerabilities.

Prevent unwanted recognition and tracking: Recognition and tracking of objects belong to the main purposes of RFID systems. Logistics applications rely on such functionality. However, from a privacy perspective, this is not always desired, especially when persons are involved. For this reason, a mechanism that allows people to decide when their RFID tags can be used for recognition/tracking and by whom is reasonable.

1.2 Reaching the security and privacy goals

In the previous section, five high-level security and privacy goals were introduced. This section explains the general approaches for reaching them.

Maintain data security: Data can be stored directly on RFID tags or in databases in backend systems. For achieving data security, it makes sense to store as few data as possible directly on tags. This means that an RFID tag should contain just a unique identifier which acts as a reference to other data stored in backend systems.

This approach offers many advantages. The RFID tags need little storage which keeps their cost low. Furthermore, potentially privacy sensitive data are not transferred between tags and readers on an insecure medium, and costly measures for protecting these data are not required. Instead, secure and flexible access control methods can be applied for accessing the data in the backend. There are also some other advantages like flexibility, interoperability, and increased speed of reading. Due to all the advantages, storing only identifiers directly on the tags and all other data in backend systems is the approach used in most RFID research. We assume the approach as basis in the following.

Prevent counterfeiting: Using the "track & trace" approach, it is possible to implement plausibility checks. By keeping a detailed object history and by storing the intended movement of items, it is possible to detect unexpected object locations that indicate fraud.

However, keeping such an object history requires a dense network of readers and standards for data exchange. Using "track & trace" with its extensive product history is also add odds with privacy requirements and does not allow for "real" security.
For preventing counterfeiting effectively without requiring such an extensive data collection, an authentication mechanism is an inevitable requirement. The authenticity of RFID tags should become verifiable to prevent tag cloning.
Prevent illegitimate access: Also for achieving this goal, the authentication ability of RFID tags is essential. If only data of authenticated tags is processed, attackers cannot enter invalid data into the RFID system. Note that there is a class of attacks called "relay attacks" [Kfir, Z. & Wool, A. (2005)] that cannot be prevented by tag authentication alone. Considerations regarding this class of attacks are beyond the scope of this text.
Cope with denial of service: Denial of service attacks cannot be fully prevented in practice. For instance, tags can be permanently destroyed by mechanical, chemical or electromagnetic means. Temporary denial of service can be performed by shielding the tags or transmitting disturbing noise. One can only try to implement mechanisms to detect such actions, provide means for sanctioning, and implement processes for recovery. For security and privacy researchers who implement new concepts and protocols for RFID communication, it is important that no additional means for denial of service attacks are introduced with the new solutions.
Prevent unwanted recognition and tracking: It is important that outsiders, i.e. potentially unwanted readers, are not able to abuse the data stored on RFID tags for unwanted recognition and tracking. Arbitrary static data, e.g. an identifier or even encrypted data, acts as a means for recognition and tracking. Even constellations of tags with different amounts of data can be used for tracking purposes.
For preventing unwanted recognition and tracking, no static data may be stored on tags. This means that a periodic change of the tag identifiers is required. The idea behind this concept is that only authorized parties can link the changing identifiers to the tag identity and the data stored in backend systems. Illegitimate parties can no longer distinguish whether two tag identifiers obtained at different times belong to the same tag or not.
Altogether, for reaching the five presented goals, three core functionalities are required for RFID tags: (unique) identification, authentication, and modification (regular changes of tag identifiers). As important constraint, implementing these functionalities should not introduce additional possibilities for denial of service attacks. *Identification* is the basic functionality required for RFID systems to operate. *Authentication* mechanisms prevents tag cloning (and therewith counterfeiting) and illegitimate access. *Modification*, i.e. a regular change of the tag identifiers, prevents unwanted recognition and tracking. RFID researchers implement these functionalities in different ways and propose various schemes.

1.3 Solution requirements

In addition to fulfilling functional requirements, RFID systems should fulfill many non-functional criteria, i.e. provide quality or have certain qualities. This section defines a set of requirements that can be used for the evaluation of an RFID system and its core components. The requirements are mostly also usable for evaluating RFID communication protocols.
Security and Privacy: The importance of security and privacy for RFID systems and the complexity of their achievement have been discussed at the beginning of the chapter. The

previous section presented the properties a system should have in order to fulfill these requirements.

Resources: Since the amount of resources needed for the realization of RFID solutions have an effect on the costs, it is important to keep the required resources as low as possible. The cost factor determines the economic incentive of the technology. As RFID tags have to be produced in oodles to be applied on everyday objects, the tag cost and therewith the available tag resources are the most limiting aspects.

Performance: The performance of RFID systems can be measured on the time needed to read a bunch of tags, i.e. to get all the relevant data. The result depends on many factors like the bandwidth of the physical communication channel, the amount of data to be transferred, the number of message roundtrips, the time for retrieving data from backend systems, the use of caching mechanisms, etc. Performance can be improved by keeping message size and number of messages small and by using caching and delegation mechanisms.

Scalability: This is an important quality for systems intended for inter-organizational or even worldwide use. The design of a system has to allow in best case an unlimited extension of users, data, and devices. There should not be any bottlenecks in the system. In practice, this requirement is fulfilled by distributing load without requiring central systems for control.

Reliability and availability: RFID systems often become part of business processes. Like with most information systems, companies and people start to rely on the operation of the technology. Failures and errors disturb business process and can thus become very costly. Therefore, RFID systems should always be available and operate reliably.

Usability: RFID systems should be calm, just like any ubiquitous computing system [Weiser, M. (1991)]. This means that these systems should not require the user's attention if possible. The RFID systems have to work for the user and ease his everyday life without disturbing or bothering him. User interactions should be required as seldom as possible, and the technology should not require a special behaviour from the user, e.g. waiting until an operation is completed.

Sustainability: In some application areas, RFID tags have a long life span. For example, RFID tags are used to identify university inventory, firm inventory, and library books. This needs consideration when implementing mechanisms that rely on cryptographic primitives. What is secure today is often no longer secure some years ahead. RFID systems have to keep up with the times. This means that new tags should be able to use up to date cryptographic primitives while older tags still use less secure ones.

RFID tags usually implement primitives in hardware that cannot be updated. Replacing such tags may be economically infeasible. It should be possible that such tags remain in operation. As they use less secure primitives, these primitives might get broken with feasible effort at some time. The impact of such a security breach should be as limited as possible, e.g. the affected tag should still be identifiable and only lose some privacy features.

Universality: In order to use RFID tags all over the world and in different applications, the tags have to be designed in a generic and application independent manner. Having the same kinds of tags reduces costs due to mass production. Having the same level of security and privacy protection everywhere relieves the users from the burden to pay attention to the level which is implemented with a particular tag. Of course, it should be possible to hold arbitrary application specific data in an RFID system and to use different cryptographic primitives. This means that a high level of flexibility should be provided with only a small number of different kinds of RFID tags.

Scope: The scope of RFID application areas varies from local to global and from intra-organizational to inter-organizational. Ideally, RFID system architectures and therewith RFID systems are able to operate on a global, inter-organizational scope.
Practicability: Many proposals regarding RFID security and privacy are of academic nature. Some proposals even only work in theory but inherently fail in practice (e.g. some protection schemes require ideal synchronization of data transmissions and/or do not consider the behavior of the physical layer). Practicability is thus a crucial requirement.
Practicability also needs to be considered with respect to the already mentioned *usability* and other requirements: Low costs, fast processing of the data, minimal user involvement, and secure handling of data are some of the problems that are, at least indirectly, linked to RFID's practicability.

2. Current RFID system architecture

This subchapter describes the common RFID system architecture. It shows that the architecture is based on the one known from other kinds of auto-id systems, like optical barcode systems. Afterwards, the general direction of security and privacy research is outlined. Overall, the subchapter shows a "mainstream direction" of RFID architecture and RFID security and privacy research.

2.1 Barcode systems as the guide

A typical barcode system is depicted in figure 2. This example shows the operation of a cash register in a retail market.

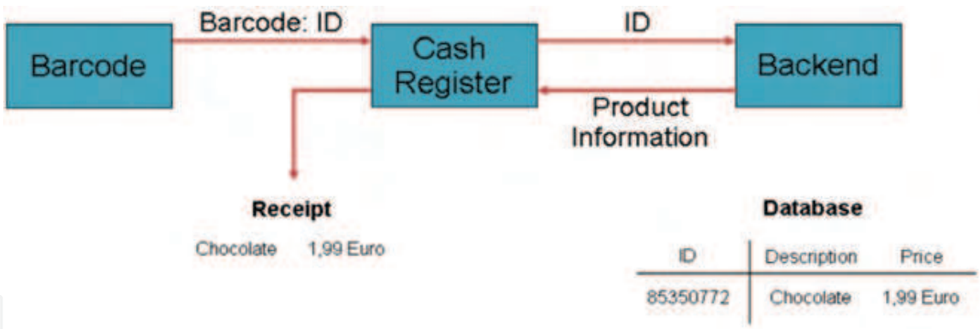

Fig. 2. Barcode system example

Optical one-dimensional barcodes provide product information via bars with different width and space between them. To read the information for a given product, the barcode of the product is captured using a barcode reader, sometimes also called "scanner". In the example, the reader is directly connected to the cash register. In a supermarket, the barcode contains an identifier for the manufacturer and an identifier for the product type. These identifiers do not provide the required information like the product price to the cash register. Thus, the scanned information is transferred to the backend of the system. The backend has a database with item information and retrieves the database record associated with the given barcode data. The database record includes information like a product description and the current product price. The product information is then transferred back to the cash register. Usually, the backend also keeps a product inventory, i.e. information on the number of items available. This information is updated when triggered by the cash

register. The cash register now has all required product information to print the customer receipt.

RFID systems have corresponding system components: RFID tags, RFID readers, and backend systems. Low-cost passive RFID tags are intended as an alternative to optical barcodes: The tags can store a certain amount of data, e.g. 128 bit. For the point-of-sale, the data forms an identifier that is structured into manufacturer, product type, and a serial number. The serial number part makes the identifier unique.

Apart from the additional serial number, RFID systems for the point-of-sale are fully compatible to barcode systems. The process that has been shown in figure 2 remains the same in such cases. Using RFID labels as a replacement for optical barcodes is therefore a simple task. Only if additional possibilities that result from the serial number shall be used, vendors have to provide new software.

Based on the similarities between barcode systems and RFID systems, figure 3 shows an "Auto-ID Triangle". The barcode or the RFID tag is the "media" on which some data, i.e. the "content", is stored. The data has a meaning which is defined by numbering schemes. The media is read using readers which generate read events that are processed. Such a "data processing" can have arbitrary forms. Read data, usually containing an identifier, can be linked to additional data that is stored in databases. The mentioned read events can be filtered, data can be linked to other data, or whatever else.

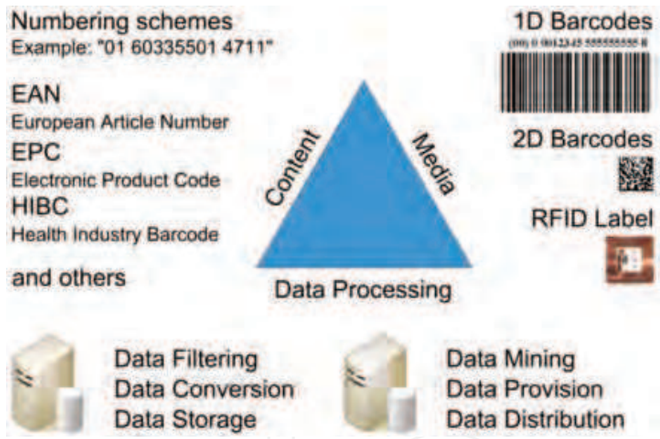

Fig. 3. Auto-ID Triangle

Note that RFID tags can have additional functionalities like sensors or smartcard-like functionality. Such additional functionality breaks the analogy between barcodes and RFID. It is thus not covered by the Auto-ID Triangle in figure 3.

Interestingly, the major limitations of auto-id systems today are within the backend systems, i.e. the data processing. This means that efficiency and productivity could be much higher if there were better backend systems. For instance, if products are processed by different companies, often each company applies its own barcode to the product instead of using already present barcodes. This is often not necessary if the reader and the backend are flexible enough. RFID tags or 2D-barcodes with their means for unique identification can make reuse much simpler because there is no possibility for identifier collisions any more.

Data sharing between companies is another aspect with room for improvement. In many business processes, there are still many manual steps that could be avoided using

appropriate information technology enabling inter-organizational data sharing. For instance, if bills had a unique identifier that could be read by an auto-id system, one could retrieve payment information automatically instead of entering the required data.
The Object Name Service (ONS) [EPCglobal (2008)] maps unique identifiers (here: Electronic Product Codes, EPCs) to additional data in an application independent manner. It operates quite similarly to the domain name system. However, it is only a first building block. For flexible and efficient inter-organizational data sharing, a lot more functionality and open standards are required.

2.2 Security and privacy research

There is an essential difference between barcode systems and RFID systems. RFID systems use electromagnetic fields or waves as data transport medium. Since this medium is easy to tap, the communication channel between RFID tags and reader needs to be secured (ref. to fig. 4). In contrast, the optical channel in barcode systems requires a line-of-sight. A barcode on an item in a bag cannot be read, whereas this is possible with RFID tags.

Fig. 4. RFID system with vulnerable communication channel

Research in RFID systems is thus concerned with the definition of communication protocols that secure the vulnerable channel between tags and readers. A lot of researchers concentrate on methods that not only provide security features but also assure privacy protection in RFID systems.
The achievement of the stated security and privacy goals (see subchapters 1.1 and 1.2) requires three basic functionalities. Protocols need to implement identification, authentication, and modification. This means that an RFID tag must be able to identify itself, to authenticate itself, and to change its identifier regularly. Many researchers propose protocols that implement these three basic functionalities in different ways, to a different extent, and in different quality. First protocols for RFID communication have been presented in 2002 [Sarma et al., (2002)]. However, the research continued in this direction, and still today (2008) new communication protocols are introduced on major conferences (e.g. [Henrici, D. & Müller P. (2008)]).
A presentation, comparison, or evaluation of the published approaches can be found, for example, in [Lehtonen et al., (2006)] with a focus on authentication and for more general approaches in [Avoine, G. (2005)]. Avoine also maintains a website (see http://www.avoine.net/rfid/) with links to publications.
Protocols have to consider the amount of resources consumed by the RFID tags. This amount has to be kept as low as possible to assure cost-effective production of a large number of tags. For this reason, the implementation of the three functionalities needs to be kept as simple as possible. This leads to avoidance of symmetrical and asymmetrical cryptographic techniques and the exclusive application of one-way hash functions in many proposals. Most requirements stated in subchapter 1.3 also apply for RFID communication protocols.

3. Reconsidering the current architecture

The common RFID architecture is based on the one known from barcode systems. Extensions are added when required. Researchers are looking for solutions that secure the communications channel between tags and readers. Regular identifier changes shall protect against unauthorized creation of movement profiles.
In this subchapter, some major deficiencies of the current architecture are presented. Afterwards it is reasoned why extensions to the architecture are not sufficient to address all these deficiencies and thus to provide a satisfying solution.

3.1 Deficiencies of the current architecture

There are several reasons why the described architecture and the proposed security mechanisms are inappropriate for today's demand. Some important deficiencies are the following:

1. There are no explicit possibilities for infrastructure sharing.
2. The proposed lightweight security protocols supporting identifier changes are not practical.
3. Most lightweight security protocols do not support delegation.
4. Tag bearers are not a part of the RFID architecture.
5. Some solution requirements like sustainability are not considered adequately.

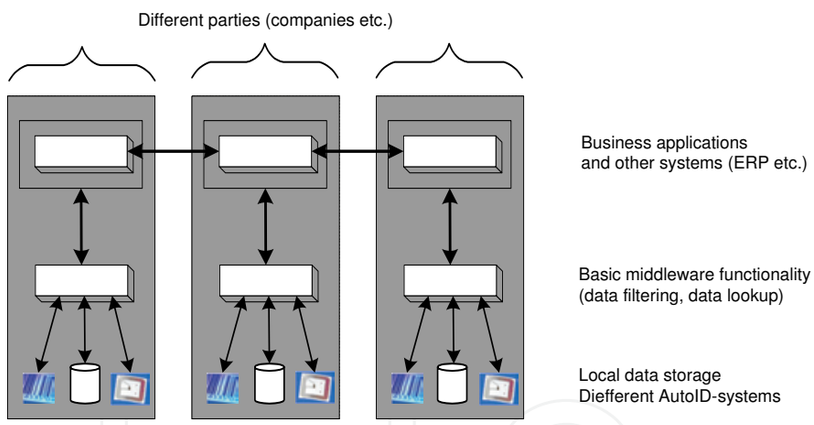

Fig. 5. Today's inter-organizational data sharing

There are no explicit possibilities for infrastructure sharing.
Each company has to build its own RFID infrastructure, i.e. install its own readers. There is no standardized way to make use of readers installed by other companies.
In practice, if a company wants to obtain read events of subcontractors, e.g. for providing item locations to customers in logistics applications, such data sharing needs to be implemented on the application layer (see figure 5). Standards for data formats evolve, but there are not enough defined interfaces and procedures so that enabling data sharing is a costly task.
The proposed lightweight security protocols supporting identifier changes are not practical.
For providing location privacy, tag identifiers have to be changed regularly. However, frequent identifier changes are difficult to provide without requiring the tags to interact with backend systems. Besides the challenge to implement a protocol with good characteristics,

regular identifier changes put high load on the infrastructure. Even without such additional load, the data produced by RFID events is a burden for networks and the backend systems.

Most lightweight security protocols do not support delegation.

Today's business processes often take place among different companies. This means that companies no longer act independently from others but have, for instance, subcontractors involved in a business process. Therefore, delegation becomes an important feature (see Molnar et al., (2005)).

To provide location privacy, identifier changes are performed. This means that subcontractors can no longer identify a tag without communication with the tag owner. For efficiency reasons, the possibility to delegate the ability to identify a tag is required.

Tag bearers are not a part of the RFID architecture.

Tag bearers are the users that carry items with RFID tags. Obviously, the privacy of such tag bearers is in danger (data security, location privacy). Nevertheless, the current architecture and therewith the RFID protocols do not consider the tag bearers at all. Instead, they regard the owner of an RFID tag (which is usually not the user carrying the tag) as trusted. For instance, if a user carries a subway ticket which might be abused for unwanted recognition and tracking, the user needs to trust the transport company which is the owner of the RFID tag on the ticket. This is not wanted. The tag bearer needs explicit consideration in the RFID architecture.

Some solution requirements like sustainability are not considered adequately.

The main research topics in the area of RFID in the past years have concerned mainly security, privacy, and resource consumption requirements. Other requirements like sustainability and scope have hardly been examined. However, they have immense significance for the quality of RFID systems. RFID systems that adhere to all the requirements stated in subchapter 1.3 are required.

3.2 Limitations in patching the current architecture

The question that arises is to what extent the existing architecture and methods can be improved to address all the deficiencies and to meet all quality requirements. Detailed analyses show some contradictory features. Using an example, it is shown in the following that just extending the current architecture does not lead to satisfactory solutions. The aim is to prove that a completely new concept, i.e. a "clean-slate approach", is required to address all the issues.

There is a conflict between systems of inter-organizational scope and the protection of privacy. This example shows the limitation of patching the current architecture. The trade-off between the two requirements is explained in the following.

As already stated, regular changes of the RFID tag identifiers are a requirement for privacy protection. Using regular identifier changes, location privacy can be provided. The idea is that the current tag identifier does not provide any information regarding the tagged item and that due to the regular identifier changes it is no longer possible to use the identifier for unwanted recognition and tracking.

However, this method poses a restriction for inter-organizational systems. Only the organization administrating the tag can also identify it because it keeps track of the identifier changes in a backend database. Only this organization can link the current tag identifier to associated data. For every other organization trying to read the tag and wanting to obtain associated tag data, the identifier appears to be just a random number. This is

necessary because the reader might also be illegitimate or even an attacker. In consequence, the identifier also appears random for legitimate readers, e.g. a subcontractor. A subcontractor cannot even find out who is the owner of the tag (see figure 6). The subcontractor might work with a huge number of other companies and now does not get the information which company is responsible. Requiring contacting all possible owners is not a scalable approach and puts too much load on the infrastructure and the backend.

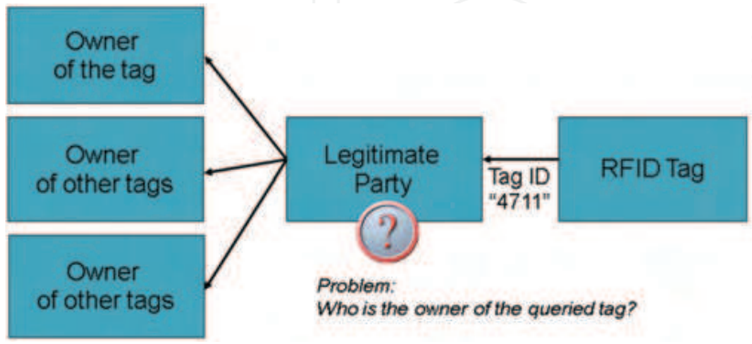

Fig. 6. Non-interpretable identifiers in inter-organizational systems

The information which organization/company is responsible for the tag may not be stored on the tag and be provided to the reader since that data can be misused for recognition and tracking purposes (at least by considering constellations). Consequently, a regular change of tag identifiers helps protecting privacy but causes problems in inter-organizational RFID systems. This means that the privacy requirement and the scope requirement run into conflict.

Theoretically, this conflict is solvable [Henrici, D. (2008)]. One possible solution to the problem can be provided by the use of pseudonymization infrastructures. They are employed for example in anonymous remailers and operate on the shared secret principle. In practice, such solutions solve one problem but bring new problems in other areas. For instance, the mentioned pseudonymization infrastructures solve the conflict between privacy and scope but require a lot of resources, lead to low performance, have scalability issues and are costly to implement.

The described conflict between privacy and scope and the possible architecture extension by using pseudonymous infrastructures is just a single example. There are many issues like the described deficiencies that need to be addressed in practice. However, the many efforts made to improve and extend the existing architecture do not seem to be able to provide adequate solutions that can fulfill all quality requirements.

4. Creating a new RFID system architecture

Subchapter 3 showed that there are many deficiencies in the current RFID architecture that need to be addressed. However, the example in the previous section showed that it will not be possible to ever meet all specified requirements in a satisfactory manner only with the use of incremental improvements. The trade-off points between some of the quality attributes require lying out a fundamentally new direction. The goal of this subchapter is to provide some considerations on how such a new, "clean-slate" architecture might be created and how it could look like.

4.1 Starting points

The toughest problem in the current architecture is probably the conflict between providing location privacy and creating inter-organizational RFID systems. This conflict was described in subchapter 3.2.

Data security demands tag identifiers that appear random. However, random identifiers do not provide information regarding the tag owner. But this would be required in inter-organizational systems. Location privacy requires a periodic change of the tag identifiers. This leads to high infrastructure load and affects the scalability of the system negatively. Even if the issues can be solved in some way, this comes at high costs.

Does this mean that security and privacy are incompatible with the economic interests and the technical needs? It seems so, a least when the current architecture is considered. The only possible way out seems to be the creation of a redesigned architecture based on new concepts.

One starting point can be found by closer consideration of the nature of privacy. When do people consider their privacy protected and when not? Answering this question is not easy. The fulfillment of their privacy expectations is of great importance to people. Meeting these expectations requires a certain degree of privacy protection. Yet, the expectations and the resulting requirements are not explicitly definable. They are context-sensitive and person-specific. This makes the modeling of privacy requirements and their technical realization a difficult task.

However, there are ways to solve the conflict between privacy protection and scalability: Humans need no total privacy protection. They are social beings and are used to give away some private information under certain circumstances. It is only important to them that their expectations regarding privacy protection are fulfilled.

Another starting point is that not all of the privacy requirements need to be addressed by technical means. The identification and sanction of a violation is often easier to implement and fully sufficient in some cases. Moreover, incentive systems can be applied. If the effort for a successful attack is higher than the expected gain for the attacker, the attacker will not perform an attack. This means, if there is no incentive for an attack, it is no longer an interesting option for the attacker. Vice versa, there is a stimulus to behave system-conform, if there is some kind of reward for such behavior.

Thus, there are also non-technical ways to implement privacy protection, e.g. via legislative or economic means. Under consideration of this knowledge it is possible to define a system architecture that fulfills the quality requirements on RFID better than the existing one.

Please note that this does not mean that technical protection schemes are not necessary. Instead, they are essential. Legislation alone does not provide adequate protection. For instance, sending unsolicited email is prohibited. Nevertheless, mailboxes are full of such email. The reason is that there are no effective technical safeguards. The possibility to sanction misbehavior is missing, too. It is thus very important that not only a kind of "pseudo security" is provided but that the sum of technical, legislative, economic and social means for providing protection deliver an effective solution.

4.2 New concepts

This subchapter provides some new concepts and outlines a new RFID architecture. Some of the concepts can also be used in other auto-id systems like optical barcode systems.

Infrastructure sharing

One of the deficiencies stated in subchapter 3.1 is the lack of explicit possibilities for infrastructure sharing in the current architecture. Each company or organization needs to

implement its own infrastructure of readers. Of course, companies can exchange data regarding read events, but such a data exchange needs to be implemented explicitly. It often takes place on the application layer and is costly to realize.

Creating a generic mechanism of infrastructure sharing is fairly simple and straightforward. First, each RFID tag needs to have an owner that shall be notified regarding the whereabouts of the tag. Second, there needs to be a policy that defines that each well-behaving reading party must contact the tag owner when a tag is read using one of the party's readers. This way, the tag owner gets a notification each time a tag is read. If the notification also includes additional information like the location of the reader, there is no difference any more whether an RFID reader is operated by the tag owner itself or by somebody else: The tag owner gets a read event each time a tag is queried.

This mechanism is very powerful. It allows companies to track items, e.g. in logistics, without requiring to define special interfaces for data exchange with each subcontractor and without operating a dense network of readers.

A tag only needs to store two pieces of information: One that enables the reading party to send a message to the tag owner (a kind of address of the tag owner). Another one is required to identify the tag uniquely. Both pieces of information together can form the tag identifier. If no other information is stored on the tags, the reading party has a strong incentive to contact the tag owner, perform the notification and request additional information regarding the tag. This is an example where a policy is enforced by an incentive.

Note that the Object Name Service (ONS) [EPCglobal (2008)] already defines a mechanism that could be used for notification purposes: Using the ONS, the reading party can contact the tag owner and get links to additional information regarding the read tag. This mechanism just needs to be adapted so that the ONS query contains information regarding the reading party.

An infrastructure sharing mechanism is highly desirable for getting the optimal results with a given amount of infrastructure hardware. It also saves costs. But if implemented as described, it also has a number of disadvantages: It puts a high load on the network infrastructure if each tag query results in a notification to the respective tag owner. It also seems bad for privacy at first sight as it makes independently operated readers to a powerful tracking device. At second sight, it only highlights a problem that is already present. If readers become networked, the tracking capability gets more powerful. But in the scenario presented here, there is also a big opportunity for privacy protection: We "just" need to solve the privacy problem once for the stated infrastructure sharing mechanism, and we get a generic solution for all users and all applications.

Tag bearers become a part of the RFID architecture

One further problem that was stated in the list of deficiencies of the current architecture is the non-consideration of people carrying RFID tags. A tag bearer is not considered in the architecture and does not have the freedom to decide when tags are read and what tag information is visible and to whom.

To solve this problem, the tag bearers need to be considered explicitly in the RFID architecture. Only this way, they get the ability to protect their privacy effectively. Figure 7 shows the integration of tag bearers into the architecture.

The procedure of reading a tag is as follows: The reading party, i.e. the party operating the reader, queries an RFID tag and obtains the tag identifier. Instead of the RFID tag, an optical barcode could be used, too. If the identifier does not provide valuable information to the reading party (which we presume), the reading party has to notify the tag bearer of the read

event and request additional information regarding the read tag. The tag bearer can now decide whether to proceed or to notify the reading party that no data is provided for privacy reasons. In case that the tag bearer decides that the request for data is allowed, he/she forwards the request to the tag owner. The tag owner can decide whether to abort or to provide the requested data regarding the tag. Thus, if both, tag bearer and tag owner, agree, the reading party obtains the information required to identify an item as well as the requested additional item information.

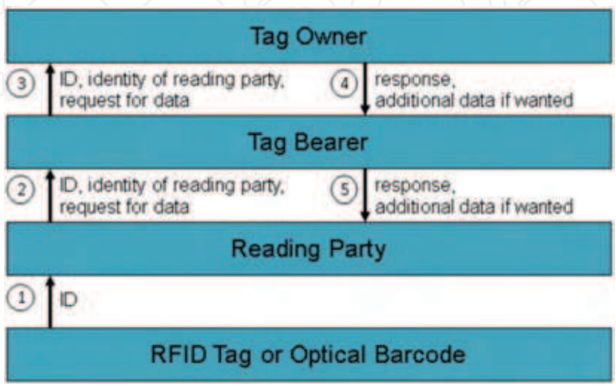

Fig. 7. Reader, tag bearer and tag owner as separate entities

The presented procedure is a straight-forward extension to the mechanism described in the *infrastructure sharing* paragraph. But it results in a number of new issues that need to be addressed.

Of course, tag bearer and tag owners cannot decide manually whether to allow tag identification or not. This would be a burden to the users. Instead, they require the ability to define policies so that most of the requests can be answered automatically.

Another issue is anonymity. For example, it should be possible for a customer to read the price of a product in a supermarket with his/her mobile phone without revealing his/her identity. This requires a neutral third party in the communication path between the reading party and the tag bearer. Another requirement is the support of changing tag identifiers for the protection of location privacy.

Reducing load while providing location privacy

There are still a lot of issues to be addressed. One major problem is the conflict between the provision of location privacy using identifier changes and the scalability requirements of inter-organizational systems. Furthermore, the *infrastructure sharing* mechanism introduced at the beginning of this subchapter puts a high load on the infrastructure by read notifications. Even more load would be caused by frequent identifier changes.

To address all the open issues, a new architecture is required. It needs to provide location privacy and needs to reduce the load on the infrastructure significantly. Some starting points were discussed in subchapter 4.2. Additionally, we require effective mechanisms for caching and delegation.

On this account, the *ID-Zone Architecture* [Henrici, D. (2008)] was created. It does no longer use the barcode-system principle but can be applied for different kinds of auto-id systems, including RFID and barcode systems. The approach is compatible with existing backend solutions.

The basic idea of the ID-Zone Architecture is the creation of zones. The physical space is separated into disjoint (non-overlapping) zones. An example is shown in figure 8. Each zone matches an administrative competency, e.g. a shop or a library.

Fig. 8. Example for the zone concept

As long as an object with an RFID tag is within a zone, the tag identifier remains constant (there are some optional exceptions for preventing industrial espionage that are not discussed here). On the one hand, this approach considerably reduces the load on the infrastructure caused by identifier changes. On the other hand, the privacy protection is slightly restricted. But since recognition within an administrative zone is often desired and can also be realized via other methods (e.g. by personnel, video cameras), this is not a relevant limitation in practice.

If a tagged object leaves a zone, the tag on the object has to identify itself with another, new identifier in the new zone so that it is not possible for an outsider to recognize that it is the same tag, i.e. the same object. This is important for privacy protection since otherwise a movement profile could be created if different zones cooperate. If a tag returns to a previous zone, i.e. a zone where it already was some time before, it is for the same reason necessary to use a new identifier, different to the former one used previously in that zone. This behavior is shown in an example in figure 9: At first, a tag has the identifier "P123:456" and enters another zone. If it returns, it gets the identifier "P123:963".

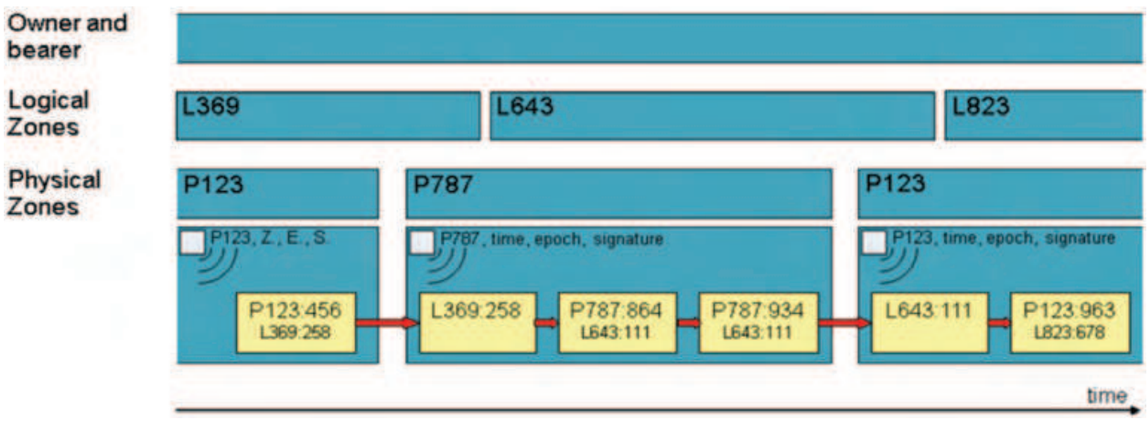

Fig. 9. Layering and example for the ID-Zone Architecture

This approach solves the conflict between privacy protection and scalability. The "logical zones" (refer to figure 9) provide anonymity for tag bearers. However, a number of new questions arise: How does a tag know from a reliable source in which zone it is? When (before leaving a zone, on entering a zone, on the first read in the new zone, etc.) and how should the change of the identifier take place?

The answer to these questions is already depicted in figure 8 but an explanation goes beyond the scope of this text. The implementation of the concepts of the ID-Zone

Architecture with appropriate efficient RFID protocols is also out of scope. More information is provided in [Henrici, D. (2008)] for the interested reader.
The message should be clear now: With new concepts and architectural changes, there are powerful possibilities for addressing the challenges stated in subchapters 1.1 and 1.3. In contrast, the current architecture is at its limits and incremental improvements are no longer sufficient.

5. Summary and research directions

The RFID technology will be an inevitable part of our everyday life in the foreseeable future. It offers various application spectrums that raise productivity, increase comfort, and open new markets. An important aspect is the consideration of the user requirements since an abandonment of the technology will not be possible for the individual. Foods, clothes, books, and many other goods will be tagged and identified with RFID tags. Therefore, designing concepts and methods that ensure security and privacy protection for systems of global scope is one of the main research goals in the field of RFID.
The challenge is great since not only technical and economical aspects have to be considered but also ethical and social ones. There need to be technical safeguards and the possibility of informational self-determination for the users. Nevertheless, the solutions have to be cheap and easy to realize. Moreover, a range of quality requirements like reliability, scalability, flexibility, openness, and sustainability have to be considered.
Besides security and privacy, there are many more research challenges. Systems need to support inter-organizational business processes. Also, the integration of people carrying the RFID tags ("tag bearers") into the system is important for providing information self-determination. In contrast, current solutions consider only the interests of the RFID tag owner (i.e. supermarkets, libraries, employers, countries, etc.). Yet, the users concerned with privacy and data protection problems are the ones who carry the tags (buyers, library users, employees, citizens, etc.). Another sophisticated problem is the provision of location privacy, i.e. protect people from unwanted recognition and tracking.
The goal of this book chapter was to advise the reader to the different challenges in the sphere of RFID systems and to point out the need of a new system architecture as a solution to the various functional and qualitative requirements.
New concepts help to address the issues. Examples are infrastructure sharing and the consideration of tag bearers as part of the RFID architecture. The sketched *ID-Zone Architecture* provides ideas on how to even resolve conflicts that seem unsolvable with the current architecture.
The presented concepts and the proposed architecture are surely no universal remedy, but they appear promising. In contrast, the current architecture appears to be at its limits so that incremental improvements will not be able to meet all the practical requirements.
The various challenges can only be addressed by heading into new directions. One of the new directions is the consideration of technical security measures in the economical, legislative, and social context. Many existing proposals concentrate on technical security measures and neglect the non-technical constraints and possibilities. Yet, non-technical measures can support the technical security mechanisms. Researchers need to start to explore the possibilities and limitations that new concepts and new architectures provide.

6. References

Avoine, G. (2005). Cryptography in Radio Frequency Identification and Fair Exchange Protocols, PhD thesis, EPFL, Lausanne, Switzerland, December 2005

EPCglobal (2008). Object Name Service (ONS) 1.0.1, Ratified Standard Specification with Approved, Fixed Errata, May 2008, available at http://www.epcglobalinc.org/-standards/ons/ons_1_0_1-standard-20080529.pdf

Henrici, D. (2008). *RFID Security and Privacy – Concepts, Protocols, and Architectures,* Springer, ISBN 978-3540790754, Berlin

Henrici, D. & Müller, P. (2008). Providing Security and Privacy in RFID Systems Using Triggered Hash Chains, *Proceedings of the Sixth Annual IEEE International Conference on Pervasive Computing and Communications – PerCom 2008*, Hongkong, March 2008, IEEE, Los Alamitos

Kfir, Z. & Wool, A. (2005). Picking virtual pockets using relay attacks on contactless smartcard systems, *Proceedings of SecureComm 2005*, Athens, Greece, September 2005, IEEE, Los Alamitos

Lehtonen, M.; Staake, T.; Michahelles, F. & Fleisch, E. (2006). From Identification to Authentication - A Review of RFID Product Authentication Techniques, *Workshop on RFID Security -- RFIDSec'06*, Ecrypt, Graz, Austria, July 2006

Molnar, D.; Soppera, A. & Wagner, D. (2005). A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags, *Selected Areas in Cryptography – SAC 2005,* LNCS, vol. 3897, pp. 276–290, ISBN 978-3-540-33108-7, Kingston, Canada, August 2005, Springer, Berlin

Sarma, S.E.; Weis, S.A. & Engels D.W. (2002). RFID Systems and Security and Privacy Implications, *Cryptographic Hardware and Embedded Systems -- CHES 2002*, LNCS, vol. 2523, pp. 454-469, Redwood Shores, CA, USA, August 2002, Springer, Berlin

Weiser, M. (1991). The Computer for the 21st Century, Scientific American, vol. 265, no. 3, pp. 94 – 104, September 1991, Scientific American Inc., New York

Development and Implementation of RFID Technology

Edited by Cristina Turcu

ISBN 978-3-902613-54-7
Hard cover, 450 pages
Publisher I-Tech Education and Publishing
Published online 01, January, 2009
Published in print edition January, 2009

The book generously covers a wide range of aspects and issues related to RFID systems, namely the design of RFID antennas, RFID readers and the variety of tags (e.g. UHF tags for sensing applications, surface acoustic wave RFID tags, smart RFID tags), complex RFID systems, security and privacy issues in RFID applications, as well as the selection of encryption algorithms. The book offers new insights, solutions and ideas for the design of efficient RFID architectures and applications. While not pretending to be comprehensive, its wide coverage may be appropriate not only for RFID novices but also for experienced technical professionals and RFID aficionados.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen