17

Data Storage in RFID Systems

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

1. Introduction

One of the advantages of the RFID technology over the still more widespread optical barcodes is the comparatively large data storage capacity. Conventional 1-dimensional barcodes can store just few bytes of data. For instance, the EAN13-code used at the point of sale in Europe stores 13 numerical digits identifying country, product manufacturer, and product type. There is no means for identifying each item uniquely. More complex 2-dimensional barcodes or larger 1-dimensional barcodes extend the amount of data that can be stored. This comes at the cost of a larger printing area as long as the readability shall not decrease.

While the amount of data that can be stored using optical barcodes is therewith limited by the available area, RFID transponders offer a more comprehensive data storage capacity. Already comparatively simple tags can store a serial number capable of identifying objects globally uniquely. RFID transponders can thus serve as a means of unique identification for different kinds of objects like clothes, foods, or documents. Transponders that are more expensive can store an even larger amount of data. For instance, additional data describing the tagged objects, a documentation of the objects' history, or even data putting the object in the context of other objects can be stored.

The question arises how to make use of the additional capabilities. What data should be stored directly on the RFID transponders and what data should be stored in databases in the backend of a system? The design decision influences many characteristics of the overall RFID system. Thus, data storage considerations are an important part in planning the architecture of such a system.

This book chapter discusses different design possibilities for data storage in RFID systems and their impact on the quality factors of the resulting system. As will be shown, many characteristics of the systems are influenced. The design decision on the data storage in an RFID system is therewith of great importance. The decision should thus be taken with care considering all relevant aspects.

Note that this book chapter relates only to RFID transponders used exclusively as data storage units. Transponders with processors, cryptographic hardware, or sensors require partially separate inspection and are out of scope.

2. Fundamentals

As already stated above, barcodes usually have only a very limited data storage capacity. For example, the International Standard Book Number (ISBN code) comprises 10 or 13

Source: Radio Frequency Identification Fundamentals and Applications, Bringing Research to Practice, Book edited by: Cristina Turcu, ISBN 978-953-7619-73-2, pp. 278, February 2010, INTECH, Croatia, downloaded from SCIYO.COM

numerical digits. Such a small amount of data is not enough to uniquely identify an item and to hold all the relevant information describing the item. The same problem exists in other numbering schemes like the European Article Number (EAN) or the Universal Product Code (UPC). These codes identify the product manufacturer and the type of a product at the point of sale. However, they cannot hold a globally unique serial number or additional data like price, ingredients, or best before date.

To cope with the pressing storage limitations, one stores all required data in databases. The data on the barcode is then taken as an index to the object's data in the database. Since the database resides on a server and the data is stored on harddisks, there are only few limitations upon the data that can be stored there. Therewith, the amount of data stored on the barcode poses no limit as long as it is capable to provide an index to the data in the database.

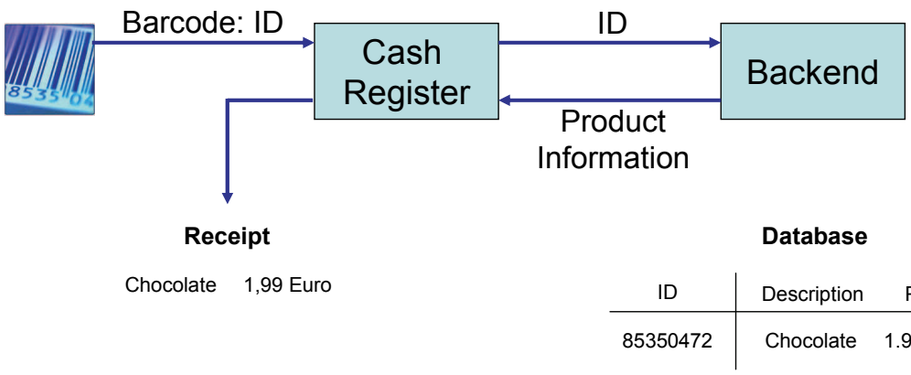


Fig. 1. Barcode system example

An example of a barcode system and the data storage in databases is depicted in Fig. 1. In the pictured supermarket scenario, the barcode ID identifies only the manufacturer and the product. A backend database contains additional product data that can be accessed using the identifier as an index. In the example, an item description of the product and the price of the product are stored in the database. In practice, the database is also used for additional purposes like keeping an inventory of the products in the store. The procedure at checkout is as follows: After the barcode is scanned on the cash register, the scanned barcode data is transferred to the backend of the system. The backend database retrieves the database record associated with the given barcode ID. The relevant data is transferred back to the cash register. Therewith the cash register has all data needed for calculating the total price and for printing the customer's receipt.

There are basically two possible data storage locations in a product identification system: directly on a barcode/transponder or within a backend database. In barcode systems, one usually has no choice: As the storage capacity of barcodes is so limited, one can only store an identifier and has to keep all other relevant data in a database. In RFID systems, there often is such a choice (cf. Fig. 2): One can store data either directly on the transponder, in a backend database, or even redundant at both locations.

Regarding the application spectrum, the storage location is practically unimportant. Remember the cash desk example: Whether the product price is read from the barcode or retrieved from the database does not matter eventually. The cash desk gets the required data, and that is what is relevant for the application. However, the different storage

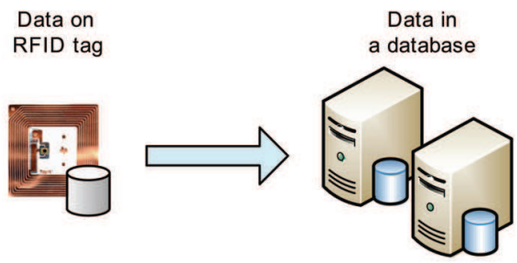


Fig. 2. Data can be stored on the RFID transponder or in a backend database

locations affect quality characteristics of the overall system differently. Such characteristics are e.g. costs, speed, flexibility, and security of the resulting system.
Usually, there are a number of data fields that shall be stored for each item in the auto-id system. For each data field, one must decide where to store it: on the transponder, in the backend database, or even at both locations. In the following subchapter, different possibilities for the realization of data storage in RFID systems, e.g. the separation of data between the transponder and the backend of the system will be presented. Afterwards their impact on different quality criteria will be discussed. Finally, an evaluation of the separate approaches based on these criteria and recommendations for their use in practice will be provided.

3. Data storage possibilities in RFID systems

The following subsections describe different possibilities of separating data storage between transponders and backend database. The different data separation possibilities are grouped into general classes. Subsection 3.1 provides an abstract description of each class. Practical examples for their application in different use cases are the content of subsection 3.2.

3.1 Technical design possibilities

In the following, general classes for the different data separation possibilities between transponder and backend are introduced. Each paragraph describes one class and is headed by a description of the data that is stored directly on an RFID transponder. All other needed data is stored in the backend of the system.

Tag with identifier and voluminous data

This class is sometimes called "data-on-tag". It intends to keep all data relevant to an object directly on the transponder and to avoid the necessity of data storage in a backend database. In this approach, all relevant product data is stored directly on the RFID transponder. The object marked with the transponder can also be identified via a globally unique identifier, e.g. the tag serial number or an identifier assigned by the application.

Tag with identifier and few additional data

In this class, a unique identifier of an object is stored directly on the RFID tag. This identifier is structured, and it comprises several parts like manufacturer and product type. Referenced by this identifier, additional data stored in the backend can be accessed. In addition to the unique identifier, a few other data fields are stored directly on the RFID chip. Normally these fields are important to the lifecycle of the tagged object.

Tag with multi-structured identifier

This scenario stores only data needed for the unique identification of the tagged object directly on the tag. All other data is stored in the backend of the system. The data identifying the object and acting as an index to data in backend databases has a defined structure. The data word subdivides into multiple parts. Each part has a particular meaning. As an example, the Electronic Product Code (EPC), which is the designated successor of the EAN code and UPC code, provides separate data word parts for the manufacturer of the product, the product type, and a serial number. Thus, the data word has a three-part structure. Each part of the structure has an interpretable meaning. The composition of these parts provides the worldwide unique identification of each product item.

Tag with minimal structured identifier having application relation

Similarly to the previous class, only identification data is stored directly on the RFID tag. Like in the previously presented class, all data describing the object is kept in databases. The difference between the two approaches is in the structure of the identifier. The structure of the data word is reduced to a technically essential minimum. The concrete structure of the data depends on the specific application context.
Identifiers having minimal structure comprise two parts. The first part specifies who is in charge of the tag. The second one provides the uniqueness of the identifier. Content of the first part could be the manufacturer of the product for example. The structure is required to provide scalability of the resulting system. This way, data can be partitioned amongst different databases: The first part of the identifier selects the database; the second part provides an index within the selected database. Within a closed system, no structure at all is required.

Tag with minimal structured identifier without application relation

This scenario is very similar to the one described before. However, the single parts of the identifier permit no inference on the application or the object qualities. The identifier again consists of two parts. The first part specifies the management organisation. It does not necessarily have any reference to the tagged object. Thus, the first part identifies neither the manufacturer of the product nor its owner or proprietary. Like in the previously presented approach, the second part is a serial number identifying the object uniquely within the management organisation. Again, the structure of the identifier provides scalability to the system. However, in this class, the components of the identifier do not reveal information about the respective tagged object.

Tag with unstructured identifier

In this scenario, the RFID tag stores only a serial number as identifier. The identifier is seemingly random and has no meaning. In a closed system, such an unstructured identifier is enough to reference arbitrary additional data stored in a backend database.
The unstructured identifier approach is only successfully applicable in closed systems. The application of tags with unstructured identifiers in a cross-organisational or even in a global RFID system is not sensible since the reader of the transponder will not be able to identify the organisation it has to contact to obtain further information regarding the tagged object. Consequently, the scalability of the system is strongly restricted. Pseudonymization infrastructures offer a theoretical solution to the problem. However, due to some drawbacks this solution is not practically interesting (see Henrici 2008).

Tag with changing identifier

Tags with a static identifier can be used for the identification of objects and therewith for the construction of traceability profiles. Such functionality is often desired, for example in logistics. However, for people carrying tagged objects, the functionality can violate privacy since indirectly people can be recognized and pursued. With a changing identifier that is still usable to identify the object in the legitimate backend, it is possible to allow only authorized individuals to recognize and pursue tagged objects and thus provide privacy protection. Possible implementations of this approach are still a field of research in RFID security (see Henrici 2008). Yet, a secure implementation requires RFID transponders that offer additional functionality than just data storage. Since such transponders are out of the scope of this chapter, changing identifiers will not be considered further.

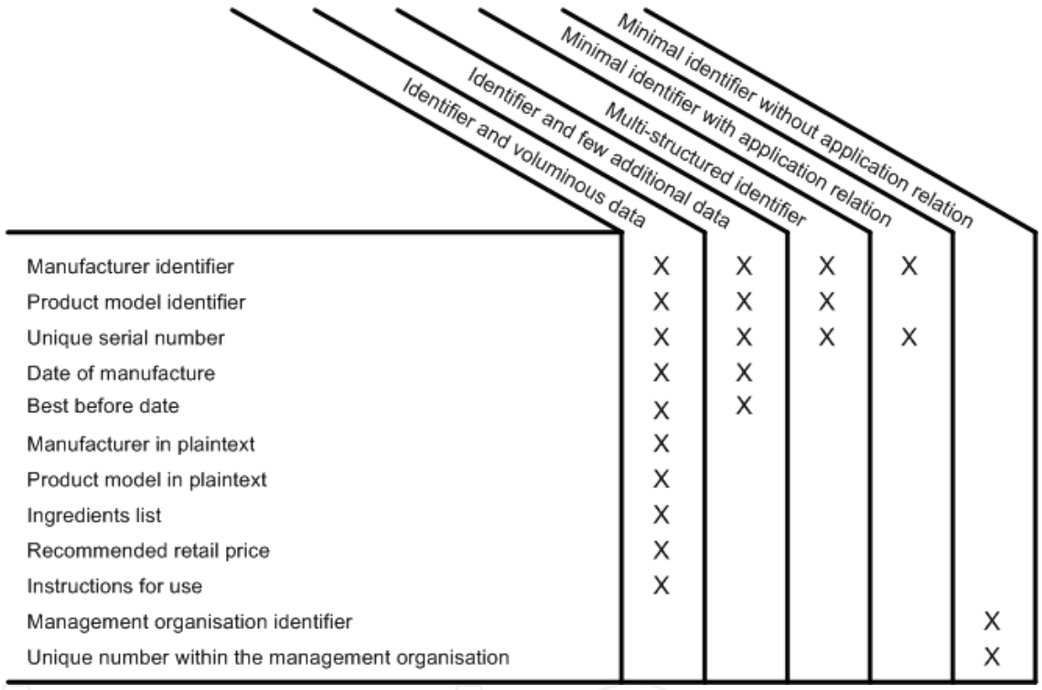


Fig. 3. Practical example: Supermarket product

3.2 Practical examples

In the following, a set of practical examples illustrates how the presented classes of different separation of data between transponders and backend behave within different areas of application. All of the examples relate to inter-organisational or even global RFID systems. In closed systems, transponders with an unstructured identifier would also be an interesting option.

For each example, a table shows which data will be stored directly on the RFID transponder. All other data relevant within the separate scenarios are found in a backend database; the data can be retrieved using the identifier read from the transponder as an index.

The total amount of data stored for a specific object is always the same. In the different approaches, the data is just distributed differently between the transponder and the backend database. A redundant storage of data both on the transponder and in the database is also

possible. However, in the scope of the considerations in this chapter only the information stored directly on the transponder is of interest. Whether this information is only stored only on the transponder or whether it is also available in the backend database is insignificant. Redundancy can be an interesting feature in some use cases though.

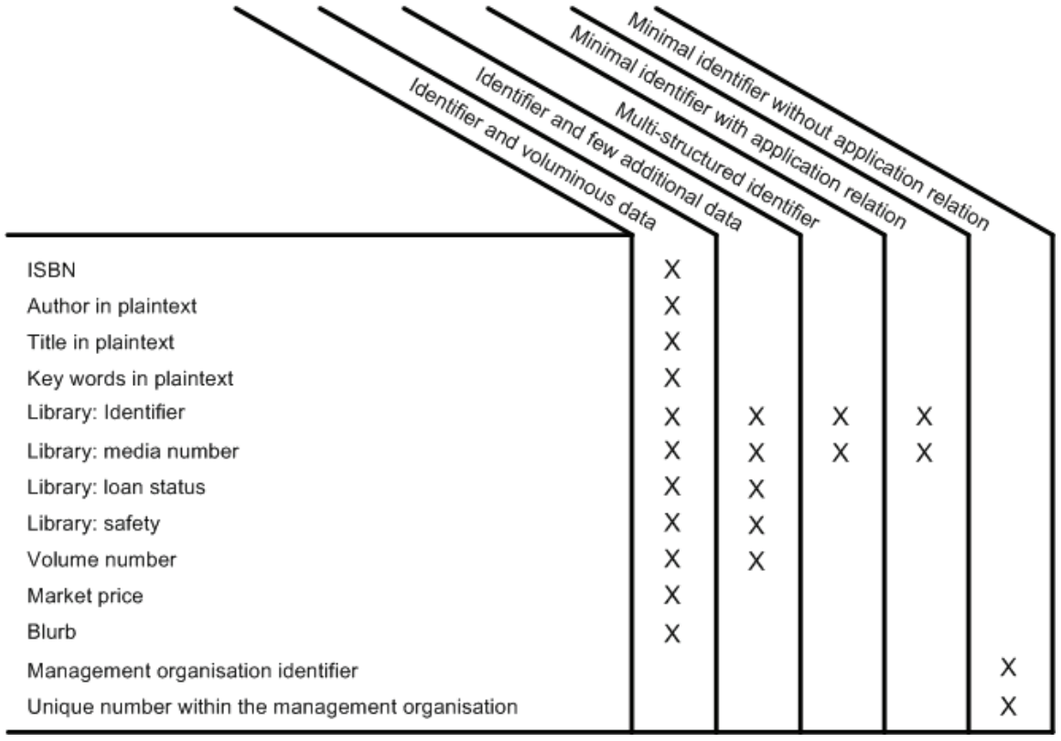


Fig. 4. Practical example: Library book

The following example scenarios are presented:

- a supermarket product (cf. Fig. 3),
- a library book (cf. Fig. 4),
- a medicine (cf. Fig. 5),
- a bus ticket (cf. Fig. 6).

4. Discussion of the different technical design possibilities

The previous section showed different possibilities to separate the required object data between the transponder and the backend. This section discusses the advantages and disadvantages that each technical design possibility has in practice. Different quality characteristics of the resulting RFID system are taken into consideration: Speed of reading and error rate, flexibility, security, privacy, and costs.

All application functionalities can be realized using an arbitrary one of the different possibilities. The application has all data available. Whether the data source is a transponder or a backend database does not make any difference regarding the functionality of the applications. However, some people argue that the data-on-tag approach has advantages for mobile applications where there is no network connection available between reader and backend. Due to the increasing ubiquitous availability of wireless and mobile networking

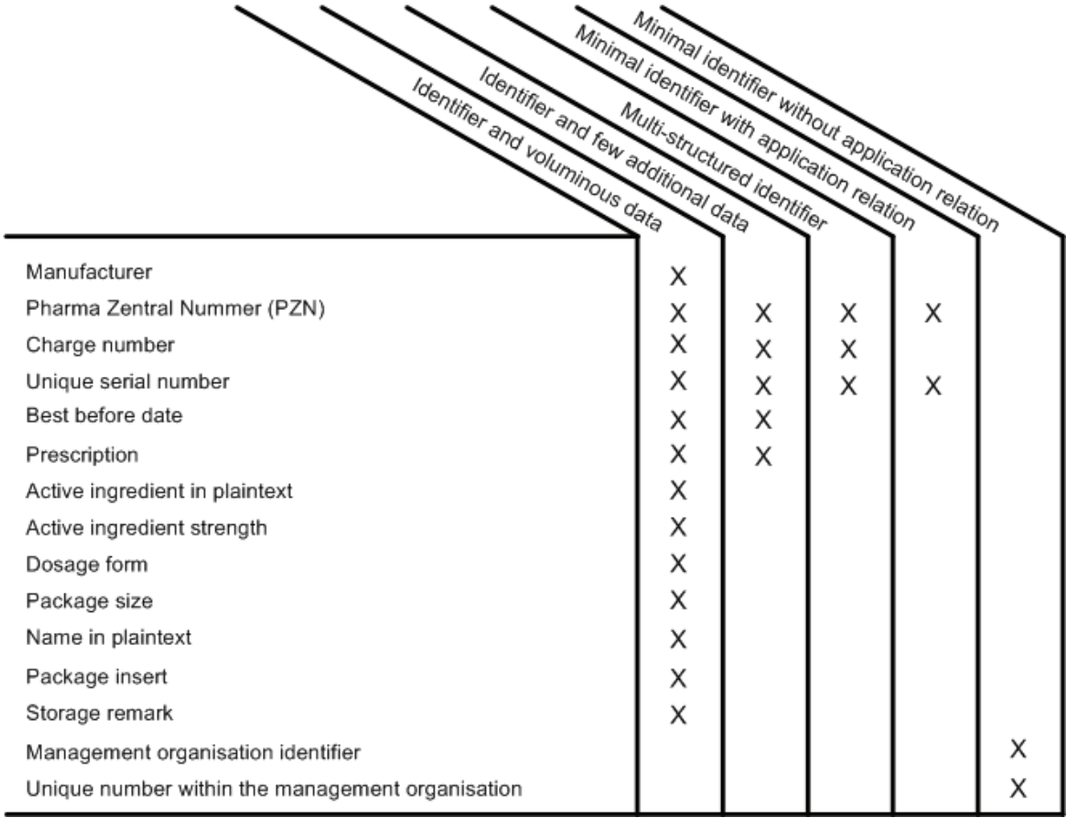


Fig. 5. Practical example: Medicine

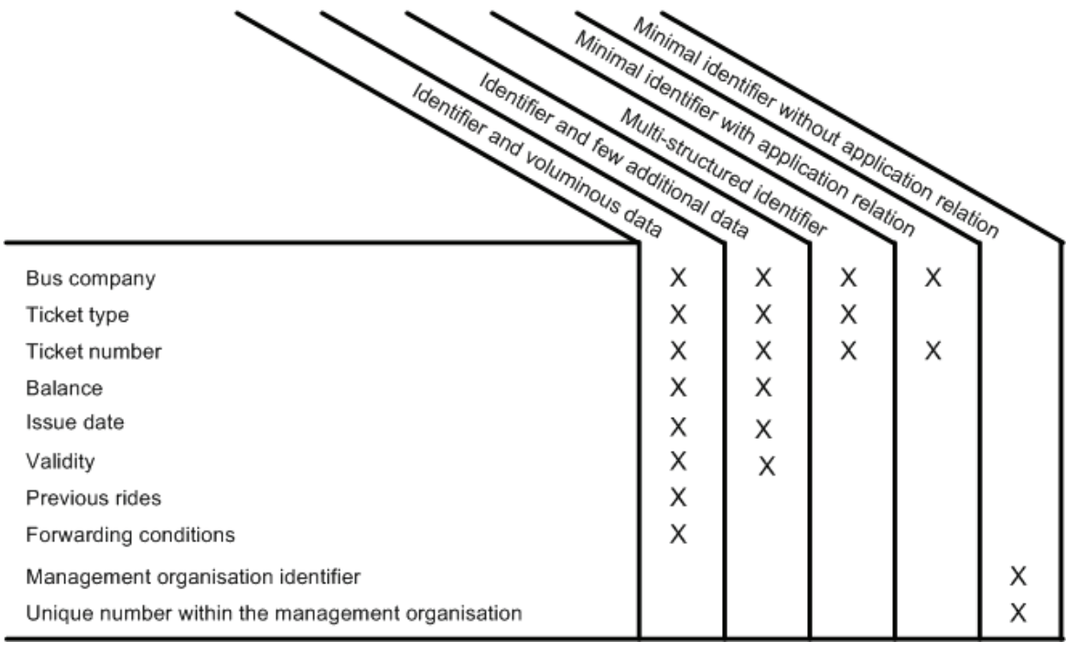


Fig. 6. Practical example: Bus ticket

and the fact that a network connection is often also required for related functionality and accessing other applications, the argument ceases importance. Moreover, other aspects like the quality characteristics presented in the following, become more important over time since business demands and user expectations increase.

4.1 Speed of reading and error rate

A high speed of reading is of great interest for many different kinds of applications. For example, on a conveyer belt as many transponders as possible are to be scanned per time unit in order to raise the throughput of the belt. When using mobile reading devices, a high reading speed is important, too, especially when bulk reading is performed. For example, supermarket consumers dislike waiting at the cash register because reading of the RFID tags is taking long. When the reading device sends out its request, a lot of tags are queried at the same time. A good anti-collision mechanism is needed but also a low time for reading a tag. It must thus be possible to read a transponder at a high speed.

Another important requirement is a low error rate. Transponders shall be detected with a high probability and their data have to be read correctly – even in disadvantageous environments. This is a very important aspect for maintaining a high data quality which is required to make the RFID technology capable of serving today's sophisticated business demands.

For both the reading speed as well as the error rate, the decisive factor is the wireless connection between transponders and reading devices. The data transfer rate and the bit error rate (BER) determine the quality of the connection. These parameters depend on the applied transmission method (e.g. frequencies, data coding) and on environmental influences.

The data transfer takes longer if the transmission rate is low. Further, for a given bit error rate on the communication channel, it is more likely that an error occurs if a greater amount of data is transferred. Conclusively, the amount of data to be transmitted should be minimized to avoid transmission errors and to achieve a high-speed of reading. In order to optimize the speed of reading and to reduce the error rate, it is advantageous to store only the data that is absolutely necessary directly on the transponder, i.e. only an identifier. Other data should therewith be kept in the backend where high bandwidths and reliable transmission channels can be provided easily.

The part of the data that is stored in a backend database needs to be retrieved from the server. Thus the reading device needs a network connection to be able to communicate with the backend. However, in current IT infrastructures such a network connection is nearly always available since it is required for other purposes as well.

4.2 Flexibility

In times of rapidly changing business requirements, companies have to adjust to new situations quickly. Therefore, flexibility is a key factor for a company's success on the market. The most flexible RFID solutions with respect to data storage are the ones that store only identifiers on the transponders and as much product data as possible in the backend.

A first advantage of exclusively storing identifiers on the transponder and of keeping all other data in backend databases is the system's compatibility with already existing barcode systems. Today, barcode systems are the most prominent solutions for auto identification. RFID transponders are expected to supplement and in many scenarios to replace the

barcodes in the future. In many years to come, both technologies will continue to complement each other and RFID tags will only be used to identify expensive products. The reason for this is that barcodes are extremely cheap, they are simple, and they do not provide that many privacy issues as RFID. In contrast, RFID transponders provide a more comfortable handling and can offer better protection against forgery. Systems that use barcodes and RFID transponder simultaneously can be easily implemented if barcodes and RFID tags are considered as different kinds of data storage while keeping the same kinds of data. This means that the data should have the same structure. In order to minimize the size of the barcodes printed on the objects, the amount of data should be minimal, i.e. just an identifier.

A second advantage of storing just identifiers on the transponders is transponder reuse and cooperation between different companies within the supply chain. When barcodes or transponders store globally unique identifiers, they can be used in a global business scenario. Several worldwide companies are involved in such a scenario. All these companies want to use the same transponders rather than to attach their own transponder to the objects. However, it may be possible that each company needs to store additional data or data that is not intended for other companies. The storage capacity of the transponders limits the additional data that each company can store directly on the transponders. Therefore, if data is stored directly on transponders, it needs to be ensured that the transponders have enough memory and that each company has the rights to access the information they need. If a company is cooperating with many others within the supply chain which is the standard scenario today, the coordination becomes very difficult if not infeasible. Just storing globally unique identifiers on the transponders is a much more practicable way to make transponder uses across companies and cooperation possible. Each company can operate a backend database, and the identifiers stored on the transponders act as an index to data stored in the backend. This way, cross-company RFID systems are comparatively easy to implement.

Systems using multiple auto-id technologies are easy to implement if data is stored in databases. For instance, barcode identifiers and identifiers on RFID transponders can reference the same data in the backend so that the different identification technologies can interoperate within the same auto-id system. Using this procedure, compatibility with existing barcode systems can be preserved. This is important in many application scenarios like the point-of-sale.

Another advantage of storing data in the backend instead of on the transponders is that in many application scenarios it is useful to be able to alter data without the transponders being in the range of a reading device. Data stored in a backend database can be accessed and altered at any time, independently from the location of the tagged object.

When an RFID transponder is read, always the current data is retrieved from the database. This results in huge advantages in certain situations - particularly when the transponders are located outside of the administrative influence. A system relying on backend databases is also more flexible because data stored in the backend can be kept up to date much easier than data stored on the RFID tag. For example, it should be avoided to store a package insert of a medicament directly on a transponder, because in the backend always the latest package insert can be made available. This is the only way to ensure that e.g. the latest information on side effects is available. This example also shows that data that is valid for many objects needs to be altered just once instead of requiring the update of all copies.

Data storage in the backend is more flexible than data storage on transponders if evolvement of applications is considered. Over time, business demands change and increase and thus new versions of applications are implemented. Updating the design often requires changing the structure of the data to be stored. Adding or deleting data fields in a database in the backend is much simpler than in the memory of numerous transponders. When changing the data structure on some transponders, others would still use the obsolete versions. This would require a version management since readers are required to handle different versions of data formats on the transponders. This increases the complexity of the whole RFID system considerably. In contrast, data structures in backend databases can be changed at an arbitrary time. The changes become valid at once, and the old data structures are no longer in use anywhere in the system. Storing data in the backend and not on transponders thus makes evolvement of applications a comparatively easy task and the implemented RFID system therewith future proof.

4.3 Security (in general)

The connection between the reading device and the transponder is wireless, using the air as transmission medium. Thus communication is public: Transmitted data can easily be intercepted. In theory, it is possible to apply cryptographic protocols to secure the transmission, but this requires the use of RFID transponders that have more functionality than just data storage and that are thus more expensive. Such tags are more powerful than cheap ones and offer functionality like cryptographic algorithms and more memory. Such functionality is considered in (Henrici 2008) and other literature. However, in this chapter we exclude these types of transponders from our discussion because in many scenarios, like in the retail trade, only cheap chips can be used. The transponders that we address in this chapter are thus able to store data (encrypted or in clear), but they are not capable of executing cryptographic operations on their own.

Storing unencrypted data on transponders exposes it to the public because attackers can intercept or retrieve the data unnoticed. As long as the transponders remain within closed and controlled areas such as a factory building, this threat can be neglected. Unfortunately, most transponders leave such closed areas during their lifecycle. Therefore, it makes sense to store as much data in the backend as possible because in this case data does not have to be transferred over an unsecured communication channel. Further, access to the data in the backend can be restricted effectively and flexibly. Arbitrary access controls to backend databases can be implemented so that every requestor for data gets just the data he is entitled to access. Such fine granular and flexible access controls cannot be implemented on transponders.

However, storing data on transponders is useful in applications where centralized data storage should be avoided. For instance, the electronic passports in many countries (e.g. Germany) currently store biometric data on transponders but do not store copies in central databases to secure the data. For such security sensitive applications, data can be stored encrypted on transponders to prevent unauthorized access. Encrypting data has the disadvantage that a key management is required. Depending on the application, such a key management becomes very sophisticated.

Another special case in which some data fields should be stored on the transponders is when there is a requirement that data shall be written exactly once and then never be allowed to be altered afterwards, not even by the transponder issuer himself. Such

"unalterable data" could be required e.g. for the protection of consumers. It is impossible to guarantee that data in the backend cannot be modified since at least the database operator can change the data. The storage of data in the backend must be avoided in these special cases.
On the other hand there is data that needs to be altered at some time of the lifecycle of an object. Low-cost RFID transponders cannot implement a stronger protection than a key/password that is transmitted in plaintext as authorization. The capability of an effective and flexible protection is thus very restricted. Such problems or even vulnerabilities are not present when having read only identifiers on transponders and storing and altering data in the backend. State-of-the-art computing power can be used in the backend for implementing flexible access control and encryption operations.

4.4 Data security and privacy

As described in the previous subsection, data stored on the transponder can be eavesdropped during communication or the attacker can use his own reading device to access the stored data. To avoid these threats, it is reasonable to store as much data in the backend as possible. An effective and flexible access control can be implemented there, and data does not have to be transmitted over insecure communication channels.
From a data security perspective, when leaving the factory, the transponder should only contain the information that is needed by other companies that process these transponders. This is the only way to avoid possible threats posed by industrial espionage and to respect the principle of data security to store no more than the absolutely required data. If just an identifier is stored on a transponder, no action needs to be taken when the tagged object leaves the company's environment. Linked data can still be available in databases so that it is available in case the tagged object returns. In contrast, when data is stored directly on transponders, some data needs to be deleted when the tagged object leaves to adhere to data security. If no copy is stored elsewhere, the deleted data is no longer available for future use.

Law

Laws regarding data security and privacy are different amongst the countries (see EPIC 2004). In many democratic countries, there are laws regarding acquisition, processing, storage and deletion of personal information. Sometimes the laws cover data that may be related to personal information or that may be linked to persons, too. The matter is already quite complex if a single country is considered. Laws and regulations varying over the countries and economic areas make things even more sophisticated.
If an RFID system is implemented, the laws and regulations of all countries in which the system shall be operated needs to be considered. To avoid different functionality and procedures in different countries, it makes sense to try to find a common denominator that is acceptable in all countries. To be safe, storage of data directly on transponders should be avoided since data on transponders is difficult to secure and since adaptation to changing laws and regulations is difficult or infeasible if many transponders are already "in the wild".

Public Acceptance

RFID technology can only unfold its benefits in all areas of life if the public does not fear it and accepts it. In the media, many different scenarios are described that show the misuse of RFID technology and how it poses a threat. Some threats are real; other threats described in these scenarios do not show exclusive misuse of RFID technology but can be said about

other systems like barcodes, too. For example, products can be associated with persons when the attacker maps the product identifiers to the consumer in a supermarket. This could both be done with barcodes or RFID tags. So, one goal when designing a RFID system should be to avoid privacy threats and to thus earn the acceptance of the public.

Data stored on a transponder can be read unnoticed; eavesdropping on the read operations is possible. Depending on the frequency, the range of a reading device can be a few centimeters up to a few meters for passive transponders. However it must be assumed that the usual range can be exceeded with specialized technology, for example by using a higher field strength. By applying technical tricks, 10 cm can easily become 50 cm (Kfir & Wool, 2005). Other scientific publications also report of even higher range extensions (Sarma et al., 2003). Note that the usual read range is only that short because passive transponders are powered by the electromagnetic field of the reading device. Passive eavesdropping is possible from much greater distances.

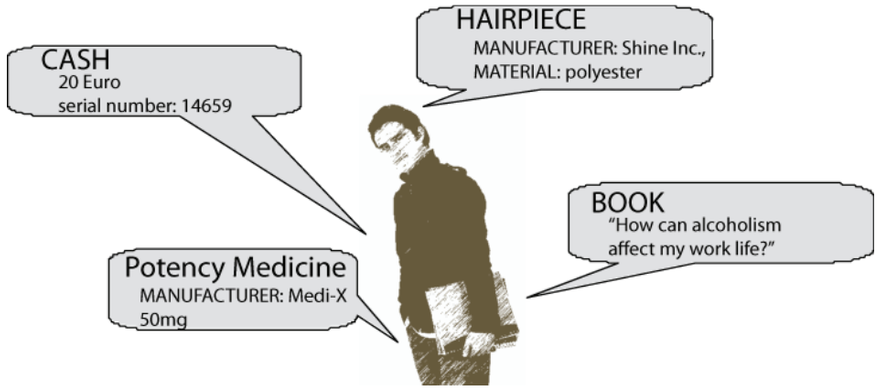


Fig. 7. Example for the violation of privacy

An example for the violation of privacy can best describe the impact of storing too many data directly on the transponder. Imagine, you could read all transponders that the person in Fig. 7 is carrying. A lot of confidential information could be retrieved, such as the health status or embarrassing details of the person's life. RFID transponders might be used for detection and prevention of banknote forgery, so a pickpocket would know if someone carried enough money worth a theft.

The privacy problem in this example originates from a combination of harmless pieces of information. Together the pieces provide a lot of personal information. The pieces of information are:

- A link between persons and objects: We see that the person carries objects.
- A link between objects and RFID transponders: The transponders are attached to the objects.
- A link between RFID transponders and stored data: The transponders store data that have a meaning.

A single piece of information is relatively harmless, e.g. the RFID transponders contain no personal data. Nevertheless, several pieces can be assembled to form a detailed image, thus undermining privacy. The data on the transponders can be linked to the person and conclusions can be drawn.

To solve this problem completely, the data on the transponders must not reveal any information that would be interesting for an attacker when linked to the person carrying it. Thus, from the perspective of data privacy, it is recommended to store as little data as

possible directly on the transponders and to take away any interpretable meaning of the data.

Even the listing of manufacturers, product key and serial numbers is too much information, as we learn from the example. Nevertheless, current plans for the point-of-sale are to equip all products with an RFID transponder that contains at least the manufacturer, product type, and serial number in the form of a multiply structured identifier. The reason is that the developers used what is the standard in barcode systems (manufacturer and product type) and transferred these concepts to the new RFID systems by just adding a serial number.

Sometimes it is argued that the identifiers used in barcode systems are just plain numbers that have no meaning to an attacker as they cannot map the numbers to the manufacturer or the product. However, this argument is misleading: firstly, the mapping between identifiers and brand and product type is known to every enterprise resource planning system in the point-of-sale so that it cannot be kept secret; on the other hand, an attacker can easily create tables with the mappings by hand. For example, for the well-known EAN-system, an official database is freely accessible (GEPIR, 2009). Additionally, there are a number of community-driven databases (see EAN-DB, 2009). It is probable that such databases will be available for the EPC (Electronic Product Code) in the near future, too.

For privacy reasons, RFID transponders should thus contain only minimally structured identifiers that preferably have no interpretable meaning. This means that a minimally structured identifier composed of an identifier of a management unit and a unique serial number provided by this unit is the best choice. Ideally, the management unit has no reference to the object whatsoever. The management unit should be neither the manufacturer nor the owner or the proprietor of this object because such information can provide clues to the nature of the product.

In the previous subsection 4.3 a special case was discussed: data that may not be altered or data that should not be stored in a central location. To hide such data, it should be stored on the transponder in an encrypted form. The necessary key to decrypt the information can be stored in the backend where it can be secured by the necessary access controls and other measures. Alternatively, the key can be printed on the object. This is done in electronic passports: the data of the holder's photograph can be decrypted using data that is printed on the passport. This protects the data from being accessed unnoticed by the passport holder.

Location Privacy

Another privacy issue arises when a person is constantly carrying objects with RFID transponders attached to them. Example objects are watches, eyewear, and footwear. Then the so-called “location privacy” is threatened: When a reading device detects a transponder several times, it is possible to conclude that it is most likely carried by the same person. This information can be used to create a movement profile or to capture consumer habits.

A related problem would occur if tire manufacturers would equip tires with transponders. Petrol stations for example could create movements profiles unnoticed by the consumers and log where and how often a consumer fills up his car and thus derive itineraries and habits. This scenario is not fictional: several years ago, a tire manufacturer has announced the equipment of their tires with RFID transponders. Consumer protests resulted in a boycott and a negative corporate image; so the plan was abandoned.

The creation of such movement profiles is made possible by using transponders that store data that is unequivocal and unchanging. This can be for example a simple identifier or arbitrary other fixed data. Even encrypted data can be misused when it does not change as

the attacker can conclude that it is the same transponder and thus the same object every time he reads the same data pattern.
Just storing unstructured identifiers that change regularly is one solution to this problem. This way, outsiders cannot determine that they are dealing with the same object. Transponders with additional functionality are required for such solutions, but these are out of scope of this chapter.

4.5 Costs

The costs of RFID systems are an important issue as far as productivity and efficiency of business processes are concerned. This includes the prices of the transponders as well as the costs of the infrastructure, i.e. the reading device and the backend systems. Operating and maintaining a system leads to additional costs.
In the previous subsections, we discussed some of the factors that have impact on the costs as well, for example, time wasted by a system that reads the transponders at a low speed. This subsection addresses the direct costs that have to be considered.
In some scenarios, the number of objects is very high. Thus transponders are needed in large quantities, especially if the transponders cannot be reused. Therefore, the unit price is a major factor of the expenses. The capabilities of the transponders determine their unit price; these include the amount of available memory, hardware circuits to compute complex algorithms or protocols, etc. The number of transponders that are manufactured also affects the unit price (small batch series versus mass production).
Consequently, transponders of the same type should be used that have only a minimal set of functionality. This enables mass production. Further, transponders that only store a globally unique identifier should be used. Then only comparatively cheap transponders with a small amount of memory are required. The structure of the stored identifier, i.e. the parts in which it is divided, may differ from scenario to scenario, but the structure does not affect the price.
The prices of the reading device are one part of the infrastructure costs. In all application scenarios, reading devices will be needed, regardless of whether data is stored directly on transponders or the backend. Additional expenses for the infrastructure encompass cost of installation, maintenance and operation of the backend system and the communication network.
If all data is stored on the transponders, a mobile reading device can read the data immediately. In this case, no communication with a backend system is necessary, and therefore the costs of the backend can be reduced. This may be considerable amount because it includes the communication system as well as the backend databases.
However, in practice, the infrastructure is very often required for other purposes as well and sometimes even already available. For example, it is often desired to transfer the data to an enterprise resource planning system where the data is further processed and statistics are derived. Therefore, there will be no extra expenses for the installation, maintenance and operation of a backend system in these cases. Then it is irrelevant regarding infrastructure costs whether data is stored on the transponder or in the backend system.

5. Conclusion

Increasing maturity of RFID technology and falling prices for transponders result in a broad acceptance and usage of RFID systems over the years. RFID technology will also be used in areas where the technology is now too unreliable or too expensive.

Enterprises and service providers have to consider different options when designing the RFID systems. This chapter discussed the question whether the architect of an RFID system should decide to store data directly on the transponder or preferably in backend systems. First, the technical design possibilities were listed and illustrated by practical examples. In the next step, the effects on quality characteristics have been shown considering the different design options.

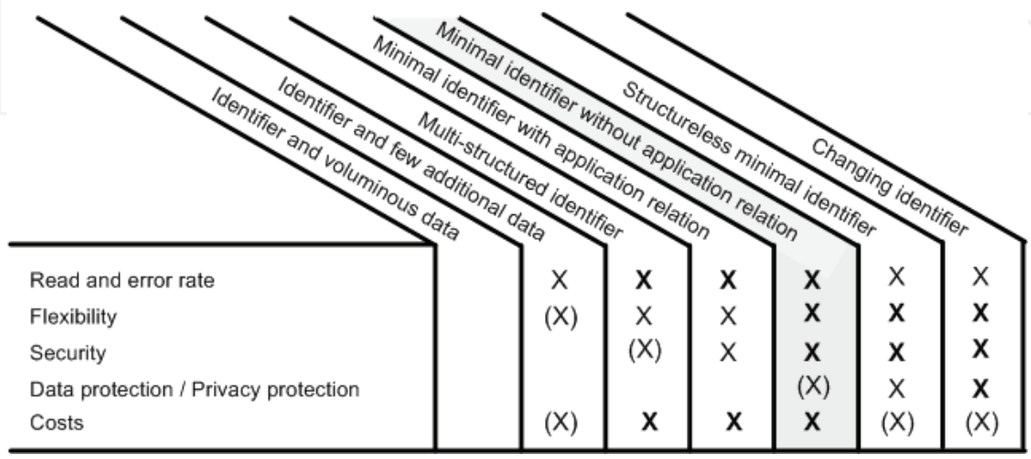


Fig. 8. Summary

Fig. 8 highlights the impact of the choice of the technical design regarding data storage on the prospective system. Plain crosses or crosses printed in brackets denote cases where the criterion is satisfied; crosses printed in bold indicate an optimal solution with respect to the criteria in question. The figure provides only the general trend and omits details and special cases.

The figure shows that the optimal solution for the protection of privacy is the one with changing identifiers. Due to the higher cost of this solution compared to other solutions, this variant will only be applied if it is required by obligation of law which cannot be expected in the near future.

The most meaningful solution is the one to only store a minimal identifier without a reference to the application context on the transponders, and all other data remains in the backend. This version enables high-speed reading so that a large number of transponders can be read in a short time. The flexibility of the backend data storage solution is advantageous in many fields of application. Modifications to existing applications are carried out relatively easily. No useful data is transmitted via an insecure communications channel. Establishing an effective access control, encryption, and other precautions in the backend is relatively simple, flexible, and cost-effective. Therewith, privacy of individuals and enterprises can be protected. The solution to only store minimal identifiers is also very desirable from a cost perspective.

Thus it is recommended for decision makers and developers to develop RFID systems in such a way that only a minimal amount of data is stored directly on transponders, i.e. a minimal identifier which has no reference to the application context. All other data can be held flexibly in backend systems. Only in special cases another approach makes more sense.

6. References

EAN-DB. 2009. *Community-driven EAN databases*
Open EAN/GTIN Database, http://openean.kaufkauf.net/
EAN search « EAN-Suche », http://www.ean-suche.de/
Codecheck, http://www.codecheck.info/

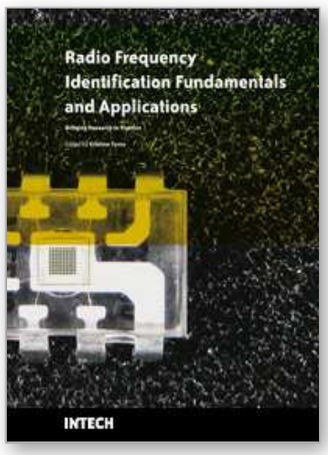
EPIC and Privacy International. (2004). Privacy & Human Rights 2004: An International Survey of Privacy Laws and Developments; Powell's Books

GEPIR – The yellow pages of GS1 – Die gelben Seiten von GS1. (2009). http://www.gepir.de/v31_client/

Henrici, D. (2008). *RFID Security and Privacy -- Concepts, Protocols, and Architectures*, Springer-Verlag, Heidelberg

Kfir, Z. & Wool, A. (2005). *Picking virtual pockets using relay attacks on contactless smartcard systems*, IEEE Conference on Security and Privacy for Emerging Areas in Communication Networks - SecureComm

Sarma, S. E.; Weiß, S. A. & Engels, D. W. (2003). *Radio-Frequency Identification: Security Risks and Challenges*, Cryptobytes, RSA Laboratories Vol. 6, No. 1, pp. 2-9



Radio Frequency Identification Fundamentals and Applications
Bringing Research to Practice
Edited by Cristina Turcu

ISBN 978-953-7619-73-2
Hard cover, 278 pages
Publisher InTech
Published online 01, February, 2010
Published in print edition February, 2010

The number of different applications for RFID systems is increasing each year and various research directions have been developed to improve the performance of these systems. With this book InTech continues a series of publications dedicated to the latest research results in the RFID field, supporting the further development of RFID. One of the best ways of documenting within the domain of RFID technology is to analyze and learn from those who have trodden the RFID path. This book is a very rich collection of articles written by researchers, teachers, engineers, and professionals with a strong background in the RFID area.

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