Security challenges for RFID key applications

Thomas Hollstein, Manfred Glesner; TU Darmstadt
Ulrich Waldmann; Fraunhofer SIT Darmstadt
Henk Birkholz, Karsten Sohr; Universität Bremen

Abstract

RFID technology is an emerging market with a wide spectrum of application domains. The introduction of RFID systems in industrial manufacturing has already been taken up more than ten years ago. Currently RFID tags are appearing in public environments like ticketing applications and retail supply chains. One the one hand mass applications will imply a break-through for RFID technologies, on the other hand new security issues have to be addressed in order to obtain an add-on benefit compared to classical barcode applications. In this contribution we address RFID security issues in general and related to selected application scenarios. At first we introduce basic RFID security requirements. Subsequently application oriented security measures are discussed for three application scenarios: automotive production, retail supply chains and anti-counterfeiting for pharmaceutical products. Finally challenges and perspectives for future improvements of security measures in RFID systems and privacy issues will be outlined.

1 Security of RFID systems

The consideration of RFID system security can be addressed on different levels: the field of security for middleware and databases has been generally addressed in information technologies and internet based systems during the recent decade. Therefore in this contribution we focus on the RFID tag to interrogator interface and its wireless information transmission. Basic principles for attacking such RFID front-end systems are among others:

- Sniffing
- Spoofing
- Replay
- Denial-of-service attacks
- Relay attacks and
- Unauthorized tracking.

Applying a combination of these basic attacks, offenders can try to clone RFID transponders, to prevent reading processes (e.g. in automated checkout systems), to obscure theft or to manipulate data in production or business processes. In order to avoid misuse of RFID technologies, both the system reliability and the system security have to be optimized. Generally the following security requirements have to be considered in the context of RFID systems:

- Functional Reliability
- Authenticity
- Confidentiality
- Integrity
- Availability
- Liability and
- Data privacy

Currently existing RFID transponders provide just very limited security functionalities. Future definitions of RFID tags as well as data and communication standards (e.g. EPC Class2) will address this issue. Therefore new methods for authentication and authorization, encryption, integrity protection, pseudonymisation, tag deactivation and prevention of unauthorized read/write operations have to be addressed in ongoing research. Since tag costs (e.g. tag complexity) have to be kept in certain limits, new effective methods for mutual authentication of transponders and interrogators have to be developed. In this context the effectiveness of the communication in a limited timeframe has to be considered. Classical methods like hashed based authentication demand a lot of computation effort on the reader side and even on the transponder side a comparatively large hardware effort is necessary. Symmetric encryption methods are not suitable, since the effort for a secure key management is comparatively high and not affordable at the required limited transponder complexities/costs. Furthermore there is a certain risk that secret keys could be revealed by reverse engineering and this in effect would compromise the whole security concept. Therefore new lightweight cryptography methods are required, including effective methods for the on-tag generation of random numbers and the computation of hash functions. Concepts as physically unclonable functions may show a way out of the security at high implementation cost dilemma. This contribution summarizes essential results of a RFID security report, supported by the German Ministry of Research and Education (BMBF), which has been published in spring 2007 [sohr07].

In the following sections we describe concrete security requirements for three application scenarios: industrial manufacturing, retail supply chains and pharmaceutical anti-counterfeiting protection. Finally we'll provide a roadmap for ongoing research and development targeting secure RFID system solutions.

2 RFID in automotive production

The RFID-technology currently used in the sector of automotive production focuses on the aspects of reliability, safety and usability in the environment of production itself. I.e., the fail-safe automation of the RFID-supported or -controlled production processes is the main concern today.

Most of the time, current implementations of RFID systems are isolated pilot applications in which there appears to be no need for extensive consideration of interoperability with other RFID systems. Privacy or security concerns are still considered as low priority as the experience with previously used technologies, e.g., 1-D or 2-D barcode labels, is considered applicable. In isolated applications, the information stored on the RFID transponders is mainly used for production process documentation. As a consequence, from the point of view of the production processes, lower demands on privacy or security arise in this sector because of its specialized and isolated nature.

The RFID technology, however, introduces new functionality. For example, high-end RFID transponders offer the possibility to store a much larger amount of data directly on the transponder itself than conventional 1-D or 2-D barcodes provide. There is a strong tendency in the automotive production – and also in the directly related sector of logistics – to store process and product information in the integrated memory of RFID transponders rather than in a corresponding backend system [vda5501].

General Trends

In the future, we expect two trends for the employment of RFID in automotive production. First, we will see a deeper integration of RFID with the existing ERP (enterprise resource planning) and production systems. As a consequence, the production processes will more and more depend on the RFID systems. This leads to higher availability and integrity requirements. Otherwise, the production process may be disrupted by manipulated data brought in by rogue RFID hardware. A typical example of such a deeper integration is to replace the currently used paper-based product and production documentation by RFID transponders.

Secondly, the future goal is a transparent deployment of the RFID technology over the whole supply chain (see **Figure 1**). By crossing the threshold between the today mostly separated installations of RFID systems (e.g., at partners of the supply-chain such as automotive manufacturers), data privacy and security become an essential prerequisite. Critical information will start to "leave the building" and adequate security measures must be made available. By becoming a widely and commonly used technology, the potential for a hostile attack on the RFID infrastructure also becomes eminent. This must be considered when developing the next generations of RFID technology.

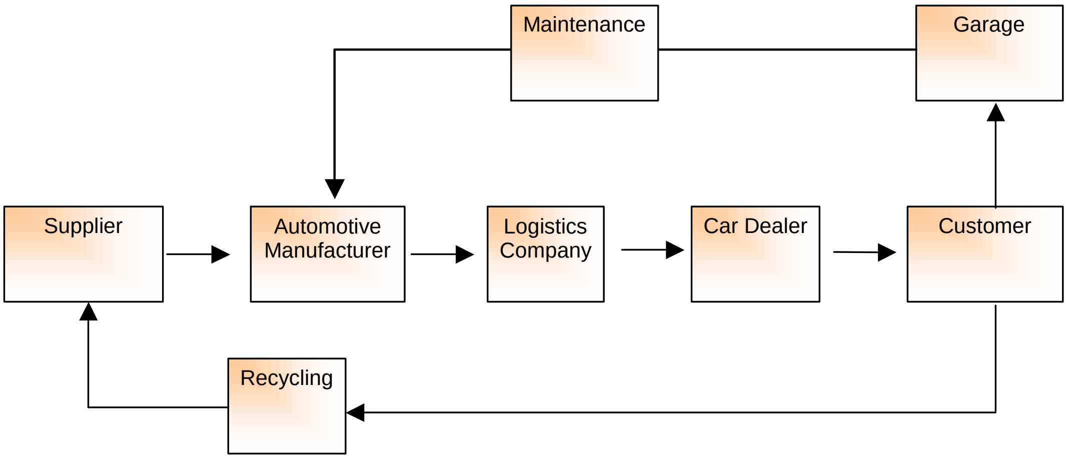


Figure 1 The supply chain of automotive production

In this section we give an overview of the requirements of the automotive production and the related sector of logistics regarding RFID technologies. We do not exclusively focus on the security- and safety-related demands, but will also give an insight into usability and deployment requirements, which arise due to the use in an industrial environment. Some examples of such demands are dimension of RFID hardware, protection of transponders from environmental influence, and various safety determined requirements.

Examples: Security in Production

Typical examples of security requirements for RFID applications in automotive production are:

- Production-relevant data such as test results should not be made available to every partner of the automotive supply chain. Due to the fact that automotive industry seems to prefer storing data directly on the tags [vda5501], a role-based authorization mechanism [sandhu96] for tags should be put in place. This way, fine-granular access control for the whole supply chain can be enforced in order to satisfy confidentiality requirements.
- An RFID-supported production process can be disrupted by bogus data brought in by an attacker. For example, the integrity of the documentation data of a production process could be violated (e.g., incorrect test and quality data of an assembly). In order to thwart such attacks, strong authentication mechanisms based upon cryptography must be implemented, e.g., tag-to-reader authentication (an unauthorized tag might be brought into the system) and reader-to-backend authentication (a rogue reader device might be installed).
- Availability is also an important security requirement for production processes. Attacks on availability, for example, may arise when tags are removed deliberately or accidentally. Under no circumstances, the production process may be disrupted in such a situation. Thus, their must exist mechanisms which guarantee a fail-safe default for the process. However, in most cases the fail-safe default in automotive production is paper-based today. Of course, this contradicts to the replacement of paper-based documentation due to a deeper integration of the RFID technology. Therefore, the development of adequate alternatives to paper-based fallback mechanisms in automotive production and logistic processes is desirable.

Challenges

To sum up, adequate security measures for RFID systems in automotive production must be derived from the security requirements such as authentication, identity management, role-based authorization and cryptography. Identifying and implementing comprehensive security measures for RFID applications for automotive production, which span the whole supply chain, remains a challenge.

Standardized technologies can ensure the achievement of these security goals and the interoperability of deployed RFID hardware. But the prospect of standardization is regarded with skepticism, specifically in the sector of logistics. Given the large number of different barcode formats used today, it is expected, that the number of different kinds of RFID hardware will be similar or even greater. To ensure interoperability between these different systems, an early definition of standards is essential: Not only for the RFID hardware itself but also for processes and protocols that can guarantee a transparent deployment of safe and secure RFID installations.

3 RFID in retail supply chains

The application of RFID technologies in business-to-business (B2B) and business-to-customer (B2C) supply chains is an emerging market. In B2B supply chains the application of RFID systems will result in improvements in many processes like OEM (Original Equipment Manufacturer) product assembling, tracking and tracing, volume handling, automated data acquisition, automated sorting, truck fleet control, delivery reliability and efficiency, product traceability and process surveillance. In B2C relations products can be equipped with unique serial numbers, providing capabilities for enhanced product service offerings. The deployment of RFID technologies in supply chain management (SCM) systems can accomplish a considerable contribution to the overall competitiveness of the retail system [michael05, levebre06]

Retail supply chain security

In the retail supply chain scenario (**Figure 2**) security measures have to be applied in order to avoid theft and the acquisition of services by false pretences. Furthermore high valued products have to be protected against product counterfeiting. Secured RFID systems have to prevent the following attacks in the delivery chain and at the point of sales [harlacher07]:

- Unauthorized information attainment (sniffing)
- Unauthorized information duplication (spoofing, replay)
- Unauthorized information modification

- Disturbance of the tag reader communication
- Relay attacks

The application of RFID tags eases the incoming and outgoing product survey in intermediate stores (distribution, wholesale) and therefore the risk of theft can be reduced and at the same time the reliability of delivery pre-packing is increased. Nevertheless, sniffing, spoofing and replay could be used for advanced approaches of theft, where RFID labels are replaced by counterfeited tags in order to direct products on different delivery paths. Additionally technical limitations of RFID readers (limited channel resources in Europe in UHF reader environments) can be exploited for manipulations in B2B chains. Furthermore the replacement of expensive original products by cheap product counterfeits with duplicated tags is a scenario, which has to be considered.

In retail stores customer manipulations like destruction of transponders or shielding of products against readout at automated cash systems have to be expected. Blocker tags could be used to prevent products from being registered at the checkout point.
Furthermore relay attacks, reading out a close by third person’s customer card for payment are imaginable.
Product counterfeiting can be prevented only by application of secured tag to interrogator communica-

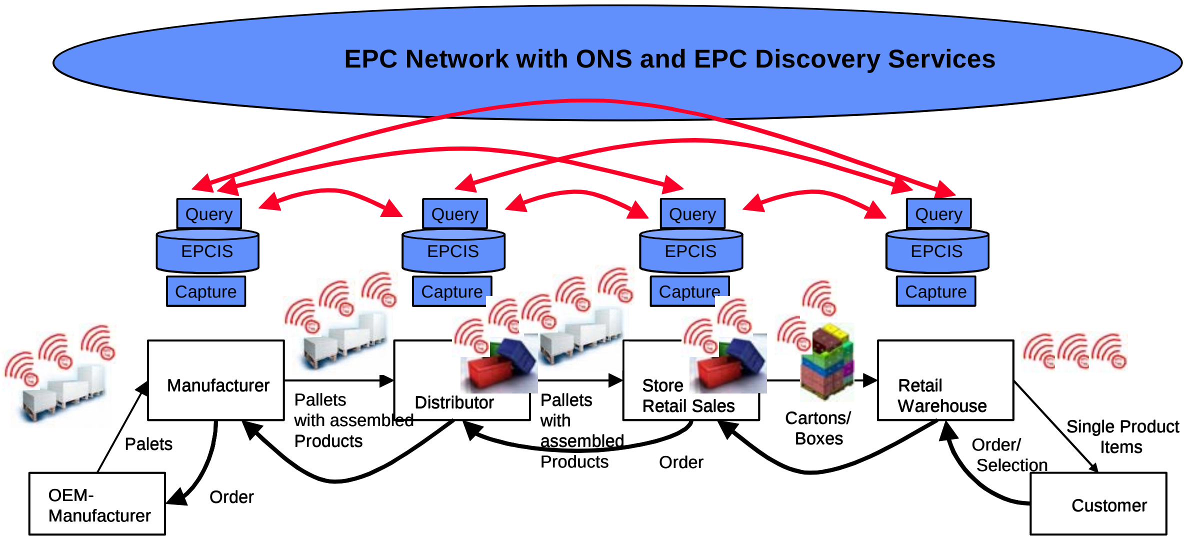
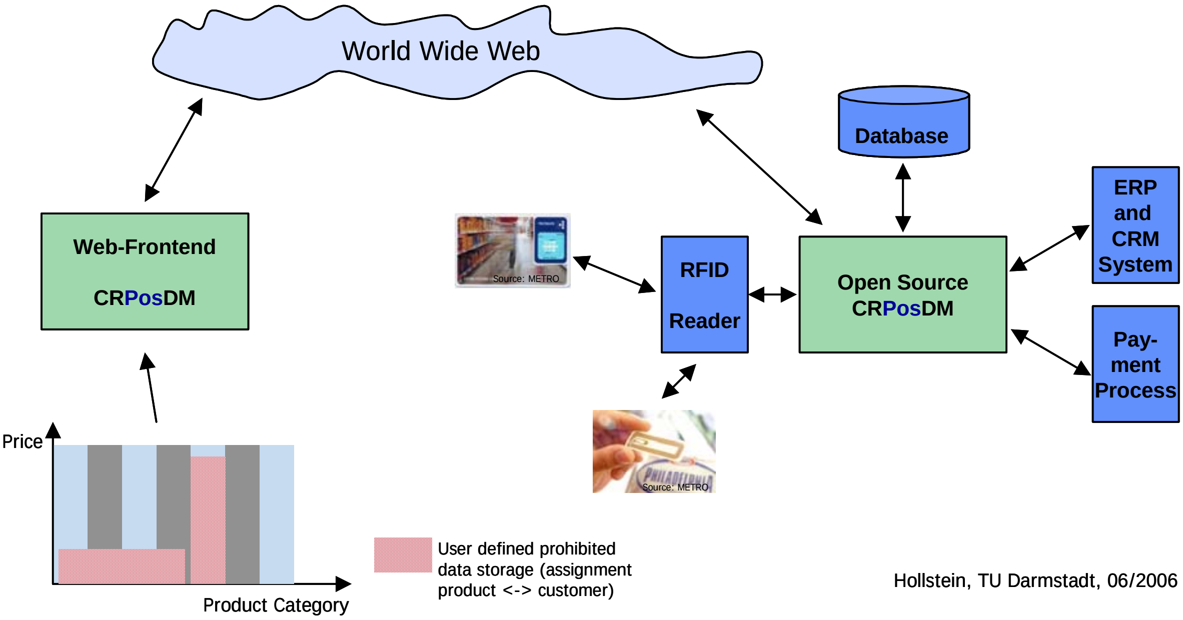


Figure 2 RFID supported retail supply chains



Hollstein, TU Darmstadt, 06/2006

Figure 3 Open-Source Point-of-Sales privacy management system

tion interfaces. The applied security measures have to be adapted to the products overall value in order to be able to provide tags at product value adequate prices. Theft can be avoided by additional optical surveillance and derived additional plausibility control at product check-in or check-out points.

Privacy issues

Privacy is a very important topic for consumer acceptance of RFID technologies. The latter can be expected, if consumers expect direct benefits from RFID product tagging and if they have extensive possibilities to influence, which individual-related data is stored or not. Tag deactivation is a minimum requirement to fulfill privacy protection.

Methods for the deactivation of tags after registration during the payment process at the point-of-sales (PoS) are suitable to reduce the privacy problem. However, in combination of with a customer bonus card a detailed profiling of the customer habits is still possible [juels03]. Even if a product ID has been deleted from a tag, but the known unique ID of a RFID tag is read at another location, it can be associated with the person who bought the product (loss of location privacy [sarma03]). Therefore additional measures for a individual customer configuration of person-related retail data structures and profiles are required. The latter has to be realized without rising unreasonable costs for retail companies. In order to come up with suitable solutions, new methods for customer-related data management have to be applied. We have developed a new scheme for Customer-Related PoS Data Management (CRPoSDM), which is shown in **Figure 3**.

This method provides the following advantages:

- The customer determines, which retail data is stored on the supplier's system. In the case, that the customer determines, that data is not stored, it can be restored/decrypted later on by applying a customer's secret key in order to receive service benefits.
- For all customers, a standard profile is generated, which defines which data (product categories, product value) is stored visibly by default.
- Via a password-secured web interface the customer can access stored person-related data at any time, having the capability to delete / encrypt it and to modify his standard profile.

In order to come up with a CRPoSDM with a high level of confidentiality at low development cost, an implementation as open-source software would be reasonable.

4 RFID in drug anti-counterfeiting

In this scenario RFID solutions are expected not only to improve the efficiency of the drug supply chain but also to protect the medicine products against counterfeiting. The WHO estimates the rates of counterfeited medicines to be 30% in developing countries and 1% in the industrial countries both with rising tendency due to an increasing quota of imported products and the Internet trade [korzilius06]. Combating counterfeits currently means information policies, special packing solutions and chemical proofs of ingredients and secret additives, which all are static measures that

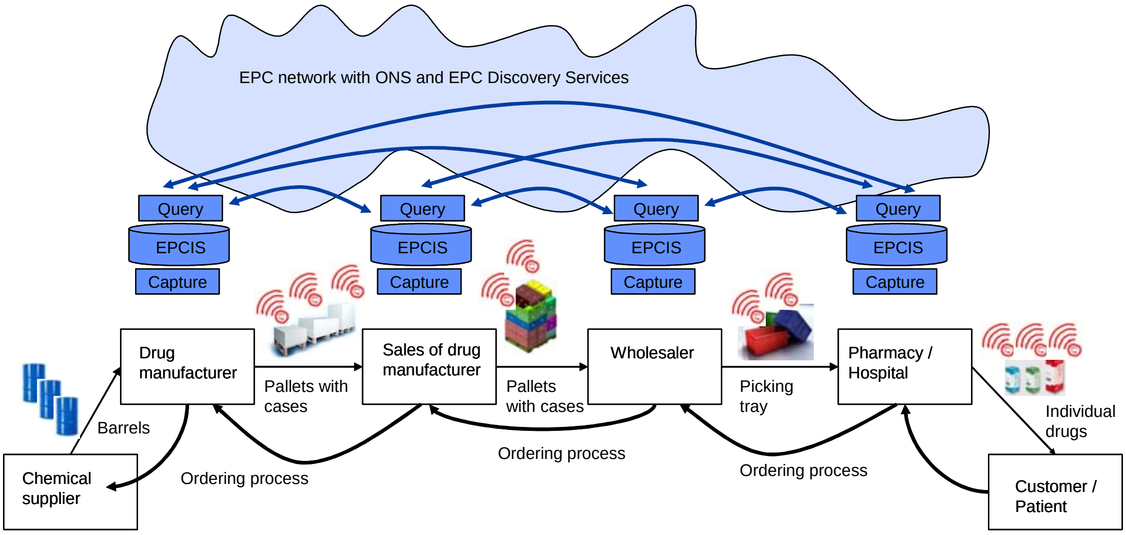


Figure 4 Drug supply chain with EPC-based RFID systems (simplified)

can professionally be imitated [platzen06]. That is why the US Food and Drug Administration recommends the dynamic use of a RFID chip and electronic pedigree for each traded drug unit [fda05]. In spite of this, the European pharmaceutical industries still push the two-dimensional barcode EAN 128 data. The German and European drug wholesalers suspect RFID of being still unreliable and inefficient for warehouse management. In general the following five obstacles are named against RFID: high costs, different incompatible technologies (frequencies), low functional reliability (reading ranges, reading rates), undefined use cases for the RFID data and the unknown effects of RFID on humans and substances. So far, there is no big effort in Europe to introduce RFID into the drug supply chains. Nevertheless, the drug supply chain seems qualified for RFID due to the favourable ratio of product value to tag costs and the presence of higher objectives such as safety [bercelon05]. The RFID concepts of EPCglobal are considered most promising [koh05, büchel06, hdma04, gs1-06].

RFID-based supply chain

Our survey refers to a RFID solution of IBM implemented as prototypes in some US drug supply chains (see **Figure 4**). The benefits are both the proof of authenticity and the possibility of track and trace of each traded packet. The system is based on the EPCglobal architecture that uses the EPC referring to locally stored information of product quality, previously passed places and other elements of the pedigree [epc-arch, epc-gen2]. Each partner of the supply chain defines what information to store in the EPC Information Services (EPCIS) and whom to grant access via XML queries over the EPC network. A minimum of data is stored in the RFID tag: the unique tag identifier entered and locked by the chip manufacturer and the EPC with the unique product serial number stored by the product manufacturer who registers the product under the combination of both identifiers. The system enforces a strict separation of data acquisition (through the RFID hardware), data query (through external access to the EPCIS) and the internal applications of the company by means of the RFID middleware. The EPCIS data are neither automatically pushed nor synchronized among the network participants but remains with their originators. Selected data is passed only on demand, but participants can subscribe to data of future events so that e.g. the shipping information is already present when the product arrives. A further principle is the use of the distributed electronic pedigree. Its separate parts have still to be retrieved from the individual EPCIS sources, but complete single-step retrieval as well as the protection of the pedigree information with digital signatures is planned.

The system supports the proof of product authenticity that is based on reading both the tag identifier and the EPC from the tag and checking whether their combination is registered or not. For that, the EPC is sent to the Object Naming Service (ONS) in order to find out the EPCIS location of the product manufacturer. Then, both identifiers are used to query the product registration. If the response was negative, the queried identifiers probably belong to a counterfeit product. The system also notices duplicates, but it is not able to indicate which of the double object the forged one is. The security is rather based on the assumption that the burnt-in tag identifier can not easily been cloned.

The industrial users of the system are still more interested in efficient and functional secure systems than in data security mechanisms. The reasons are the desired limitation of costs, the hard functional requirements at the air interface coming from high line speeds, heterogeneous materials (fluids, metals) and packing formats in the pharmaceutical industry. Which frequency (HF or UHF) should be used on package level is still an open question and should further be investigated [philips04, adt06, odin06, magellan06]. The described RFID system uses low-cost HF tags on packet level and UHF tags on the level of cases and pallets.

Further security requirements

The following considerations may clarify that the data security of the system should be improved. With regard to the given system a counterfeiter might be able to listen to the tag-reader communication or to actively read valid tag data, in order to clone tags and use them for forged products. Every reader that supports the air interface protocol usually can read the EPC data on low-cost tags. Forgers may get access to freely programmable chips.

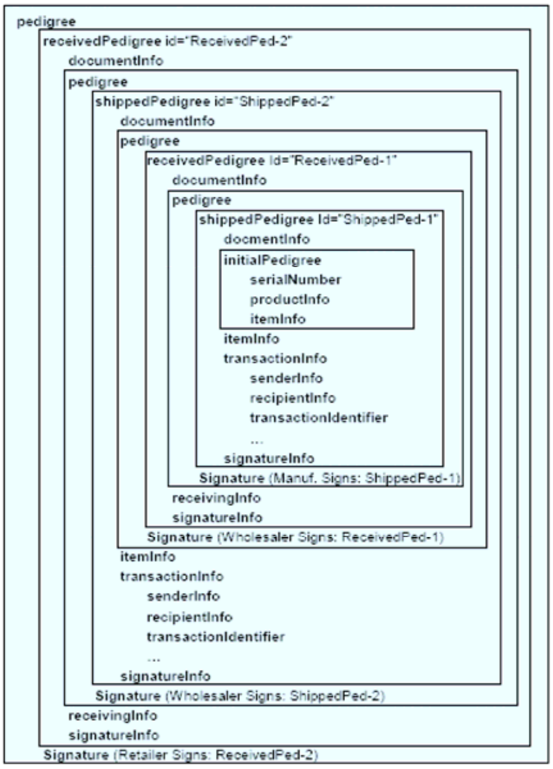
Besides querying the combination of identifiers, the electronic pedigree can be used for plausibility checks. However, the pedigree still does not ensure sufficient security against product forgery since the data may be authentic but could be a copy or be referenced by several counterfeit packages under the same original EPC. Furthermore, all distributed pedigree information remains in its original location. A corrupt originator could manipulate the information after issuance without being noticed by the other participants. Another weak point of the anti-counterfeiting system could be the unsecured connection between tag and product: an original tag may be removed from the packing of an expired or used up product and attached to a counterfeited drug.

Required security measures

Therefore, a secure solution against counterfeiting should include the following measures [inaba06, lehtonen06, lehtonen06a, duc06]:

1. Proof of authenticity of tag identifiers (as it is already realized)
2. Proof of authenticity product origin by a complete and extensible pedigree document
3. Proof of authenticity of the tag by a cryptographic authentication
4. Proof of product authenticity and right connection of tag and product

The assignment and registration of tag identifiers with the drug manufacturer is required for the first proof. The identifiers are also part of the electronic pedigree (second proof) whose requirements are described in [harrrison06]. In contrast to the distributed pedigree information used in the IBM solution an extensible pedigree is sent as a whole document along with the product and is signed over by each receiver, so that it cannot be changed after issuance by unreliable wholesalers introducing forged products. This kind of pedigree is already defined by EPCglobal [epc-pedigree], see example in **Figure 5**.



Source: [epc-pedigree]

Figure 5 – Structure of an EPC pedigree (example)

For the third proof only a strong authentication of the tag based on a challenge-response protocol using secret keys within the tag is considered highly effective against counterfeiting and tag cloning. Therefore, the tag needs a cryptographic unit similar to microprocessor chips. However, the required restriction to low-cost tags first of all restricts the cryptographic possibilities. The legal regulations on e.g. power radiation and allowed frequencies restrict the computation times and power consumption needed by a cryptographic tag. The aimed overall performance of the system sets its own limits to time-consuming cryptographic operations. The power consumption can be reduced by an improved chip design [rabaey96], but the 5,000-10,000 electronic gates of today's low-cost tags (offering maximum 3,000 gates for security functions) are hardly enough for common cryptographic algorithms like DES, AES, ECC or RSA [yu06].
Therefore, cryptographic authentication methods that go with low-cost tags are needed. The methods of lightweight and minimalist cryptography may be efficient for the tag but are complex in terms of key distribution, data synchronization or server access [yu06, ranasinghe06]. Most of these mechanisms seem unfeasible in an open supply chain with an unknown set of tags. The search for new methods e.g. in the fields of Physical Uncloneable Functions (PUFs) and Physical One-way Functions (POWs) to replace cryptographic keys or One Time Codes to use simple XOR encryption on the tags may be promising on a long-term basis. PUFs utilize minor material differences that result from uncontrollable or unknown variations of the manufacturing process. An example is a PUF circuit that shows a characteristic response from each chip when given a certain input. These characteristics are similar to secret keys but unlike keys can not be copied. Each tag can be authenticated by giving its individual PUF response [ranasinghe06a]. The use of POWs is another alternative to storing keys on insecure hardware. One solution uses a laser beam as an input to an optical medium that consists of a microstructure with randomly embedded particles. This operation results in a reference pattern that can be mapped to an individual bit string [ravikanth01]. Finally, One Time Codes would be perfect for low-cost tags since only the simple XOR bit operation is needed to encrypt and decrypt data. The security of this cipher is surpassing as long as the code is really secret, random and used only once. Research on generation and synchronization of these codes is needed for future low-cost solutions [ghosal06].

For the fourth proof (product authentication) the tag has to be affixed or embedded into the product. Counterfeiting is already made difficult on the basis of the tag and tag authentication. But also the connection between tag and packaging, the product itself must be verifiable intact. Therefore, next to the tag authentication an authentication of the product itself or at least of its packing is required to verify that the authenticated tag truly belongs to the claimed product. New mechanisms should combine physical security features (e.g. tamper-proof packing, use of tag inlays, optical methods) with RFID systems, e.g. by introducing sensor-created events. A manually operated product authentication (e.g. based on machine-readable product features like barcode, printed serial number or tag identifiers, or hologram) in the pharmacy may complete the solution against counterfeiting. For this purpose, images and individual information about the product item may be part of the electronic pedigree.

Further research topics

The pharmaceutical industry is considered kind of pathfinder for the introduction of RFID on product item level. According to an economic survey [vdc06] 65% of the US commercial users in the sections consumer goods, retail and health wait and see the RFID deployment in the drug supply chains. Research should focus on low-cost tags though not restricted to requirements of EPCglobal. Fields of research are e.g. the interoperability of RFID components, the improvement of RFID hardware (especially UHF tags and readers), the development of adapted cryptographic methods and the creation of application-specific security protocols for product authentication. The development of sensors for passive tags is a long-term objective including energy harvesting (through movement, light, differences in temperature, Piezo-effect, pressure) and signaling improper product changes to the system. Efficient offline authentication methods are needed [tsudik06]. A promising combination of physical fingerprints (on basis of PUFs), digital signatures and ECC authentication is presented in [tuyls06].

5 Technological Roadmap

RFID Security Design

A significant obstacle to the introduction of RFID is the lack of technical guidelines and application-specific standard solutions (best practice scenarios). RFID applications must be tailored to their application context by defining use cases and carrying out extensive test-runs. A targeted research and development in the following fields may help to improve the required technical bases.

RFID hardware

Reliable tags on physical level are a substantial condition for the security of RFID systems. Tags must be optimized regarding dielectric fluids and metals, temperature tolerance, electrical influences as well as mechanical load. A physical integration of tags into production parts requires new manufacturing processes (e.g. casting integration) of RFID tags. In many applications a parallel use of different frequencies (HF, UHF) will be required. Which frequency is most suitable in which usage environment has to be investigated independently from the respective hardware manufacturers. Multi-standard readers and security concepts for multi-reader environments are needed. The integration of sensors into RFID systems will improve the system reliability, e.g. by automatic detection of manipulation and recovery of RFID malfunctioning.

Cryptographic functions

The development of hardware-efficient cryptographic functions for low-cost tags is an important target of research. Furthermore, conventional algorithms must be optimized for limited resources. In some application contexts efficient offline authentication methods are needed, in order to be independent from a time-consuming access to network or backend systems. A long-term and promising research field is the replacement of cryptographic keys by low-priced physical and technology-integrated fingerprints (e.g. on basis of PUFs, POWs and One Time Codes) of the chip which should be inseparably connected to the product or the packing. Fingerprints are conceivable also for ultra low-cost tags, which are developed on basis of conducting polymers printed or integrated into product materials. PUFs and POWs based fingerprints have enhanced anti-cloning characteristics compared to cryptographic keys that can be copied. The integrated secret fingerprints would be destroyed by manipulation and cannot be determined even by reverse engineering or side channel attacks. The security analysis of published and proprietary protocols of commercially available RFID hardware is a further necessary research topic. Besides, procedures for a safe deactivation and reactivation of tags are needed not only in retail trade, but also e.g. in automotive logistics, particularly if confidential production data are stored on the tags.

System integration and security

Interoperability is essential for open enterprise-spreading RFID systems. Standardization is needed regarding the organization of data storage (either only in middleware or only on the tag or on several places). There is a further need of standardized data structures for product data and security information in tag and middleware. Standardized connections of RFID systems to ERP applications as well interoperability of services of different registration authorities (second source principle) is necessary. Future research projects should also analyze weak points of software components (reader operating systems, RFID middleware), in order to close security gaps. A development of security standards criteria for RFID technologies will be a substantial step on the way to overall secure systems. Methods for a formal description of complex RFID-supported processes should be developed for validation and verification of RFID system security. Reference models for different reader configurations and different piles of tagged products with dielectric materials may help to improve reading rates. Instead of adapting the RFID components to interfering packing materials, which has its physical limits, in the other way the packing may be modified to become RFID-friendly. Process disturbances should be recognized automatically, in order to be settled during the on-going processing. In particular the effects of small losses should be examined in a complex dynamic system as it is realized in a RFID-supported supply chain of consumer goods.

Identity and authorization management

Many research questions in the fields of organizational security management of RFID systems still exist. In particular procedures of a scalable management of passwords and cryptographic keys are to be developed. The key management in the RFID application scenarios of consumer goods is probably very complex. If a differentiable access control for tags is to be used, different cryptographic keys must be generated and managed. The key management is generally an unsolved problem in the area of RFID security, especially if product data are stored in the tags rather than in the backend. With employment of RFID throughout the supply chains an unknown and changing number of e.g. suppliers, manufacturers, wholesalers and customers will be involved. Nevertheless, the tags must be as economical as possible, so that the deployment of RFID will pay for itself. In all scenarios considered in the study [sohr07], the pursuit of tagged products throughout the supply chain is important. For this purpose a scalable and efficient identity and access management has to be established. Such a federative identity management makes a transparent authentication of individual partners possible. Which information (attributes) is needed for the individual identities of a RFID-supported supply chain, is still an open question. In particular procedures are to be developed, in order to define suitable roles and authorizations for the different supply chain partners. Existing standards (e.g. Liberty Alliance, SAML, LDAP, PKI) may be combined with RFID technologies, in order to manage the enhanced number of users and policies across technical and organizational system borders.

Privacy Protection

New Methods for ensuring customer and staff privacy have to be developed. By randomizing tag replies location privacy can be gained. In accordance with the development of new security measures, methods for the secure assignment of tag ownership have to be evolved. Based on new open source concepts, modules for trusted, standardized and customer defined handling of person related data at the point-of-sales in retail stores can evoke new potentials for trusted customer relation management systems.

6 Bibliography

[adt06] ADT/Tyco Fire & Security, Alien Technology, Impinj, Intel, Symbol, Xterprise: RFID and UHF: A prescription for RFID success in the pharmaceutical industry, White Paper, June 2006

[bercelon05] A. Stiehler, T. Wichmann: RFID im Pharma- und Gesundheitssektor, Berlecon Report, Berlin 2005

[büchel06] P. B. Büchel, O. Platzen: RFID-Technologie zur Verhinderung von Arzneimittelfälschungen, Pharm. Ind. 68, Nr. 10, 1153-1157, 2006

[duc06] D. N. Duc, H. Lee, K. Kim: Enhancing security of EPCglobal Gen-2 RFID against traceability and cloning, Auto-ID Labs Information and Communication University, White Paper, 2006

[epc-arch] EPCglobal: The EPCglobal Architecture Framework, Final Version, July 2005

[epc-gen2] EPCglobal: EPC Class-1 Generation-2 UHF RFID Protocol for Communication at 860 MHz – 960 MHz, Version 1.0.9, January 2005

[epc-pedigree] EPCglobal: Pedigree Ratified Standard, Version 1.0, January 2007

[fda05] Combating Counterfeiting Drugs: A Report of the Food and Drug Administration Annual Update, US Department of Health and Human Services, 2005

[fleisch05] E. Fleisch, F. Mattern: Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis. Springer-Verlag, Berlin 2005.

[ghosal06] R. Ghosal, M. Jantscher, A. R. Grasso, P. H. Cole: One time codes, Auto-ID Labs University of Adelaide, White Paper, 2006

[gs1] GS1-Germany: www.gs1-germany.de

[gs1-06] GS1 Germany: Fälschungssicherheit per EPC, Über EPC und EPCglobal-Netzwerk Warenechtheit gewährleisten, März 2006, Online available: [gs1]

[harlacher07] Harlacher, F.: Untersuchung der Sicherheit von RFID-Technologien und –Systemen, Studienarbeit, TU Darmstadt, FG Mikroelektronische Systeme, 2007 .

[harrison06] M. Harrison, T. Inaba: Improving the safety and security of the pharmaceutical supply chain, Auto-ID Labs, White Paper, 2006

[hdma04] Healthcare Distribution Management Association (HDMA): EPC and Healthcare Distribution: Current State of the Industry, White Paper, November 2004

[inaba06] T. Inaba: EPC System for safe & secure supply chain and How it is applied, Auto-ID Labs Keio University, White Paper, 2006

[juels03] R. Juels, R. L. Rivest, M. Szydlo: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, ACM 2003, online verfügbar unter http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/blocker.pdf, Zugriff am 18.12.2006

[koh05] R. Koh, T. Staake: Nutzen von RFID zur Sicherung der Supply Chain der Pharmaindustrie, in [fleisch05]

[korzilius06] H. Korzilius: Arzneimittelfälschungen: Globale Lösung für ein globales System, Deutsches Ärzteblatt 103, Ausgabe 48 vom 01.12.2006

[lefebvre06] L. A. Levebvre, E. Levebvre, Y. Bendavid, S. F. Wamba, H. Boeck: RFID as an Enabler of B-to-B e-Commerce and its Impact on Business Processes: A Pilot Study of a Supply Chain in the Retail Industry, Proc. of the 39th Annual Hawaii International Conferences on System Sciences (HICSS) 2006, S. 104a, Hawaii, Jan. 2006.

[lehtonen06] M. Lehtonen, T. Staake, F. Michahelles, E. Fleisch: The potential of RFID and NFC in anti-counterfeiting, Auto-ID Labs ETH Zürich und Uni St. Gallen, White Paper, 2006

[lehtonen06a] M. Lehtonen, T. Staake, F. Michahelles, E. Fleisch: From identification to authentication, Auto-ID Labs ETH Zürich und Uni St. Gallen, White Paper, 2006

[magellan06] Magellan technology: A comparison of RFID frequencies and protocols, White Paper, March 2006

[michael05] K. Michael, L. McCathie: The Pros and Cons of RFID in Supply Chain Management, Proc. of the International Conference on Mobile Business 2005; S. 623-629; July, 2005.

[odin06] ODIN technologies laboratories: Pharmaceutical item level RFID: Battle of the frequencies, White Paper, March 2006

[philips04] Philips, TAGSYS, Texas Instruments: Item-level visibility in the pharmaceutical supply chain: A comparison of the HF and UHF RFID technologies, White Paper, July 2004

[platzen06] Oliver Platzen: Die Eignung eines Auto-ID-Systems zur Reduzierung von Arzneimittelfälschung im Auftragsabwicklungsprozess zwischen Hersteller und Handel in Deutschland, Diplomarbeit Uni Regensburg, 3.2.2006

[rabaey96] J. Rabaey, M. Pedram: Low-Power Design Methodologies, Kulwer Academic Publishers, 1996

[ranasinghe06] D. C. Ranasinghe, P. H. Cole: Security in low cost RFID, Auto-ID Labs University of Adelaide, White Paper, 2006

[ranasinghe06a] D. C. Ranasinghe, P. H. Cole: A low cost solution to authentication in passive RFID systems, Auto-ID Labs University of Adelaide, White Paper, 2006

[ravikanth01] P. S. Ravikanth: Physical One-Way Functions, Massachusetts Institute of Technology, March 2001

[sandhu96] R.S. Sandhu, E.J. Coyle, H.L. Feinstein, C.E. Youman. Role-based access control models, IEEE Computer 29(2), 38-47, 1996.

[sarma03] S. E. Sarma, S. A. Weis, D. W. Engels: Radio Frequency Identification: Security Risks and Challenges, RSA Laboratories Cryptobytes; Vol. 6, No. 1, Spring 2003.

[sohr07] K. Sohr, T. Hollstein, U. Waldmann: Technologieintegrierte Datensicherheit bei RFID-Systemen, technical report, ordered by report, funded by the German Ministry of Research and Education (BMBF)(Kz. 16SV3505), May 2007

[tsudik06] G. Tsudik: YA-TRAP: Yet another trivial RFID authentication protocol, IEEE conference paper, March 2006

[tuyls06] P. Tuyls, L. Batina: RFID-Tags for Anticounterfeiting, CT-RSA 2006, LNCS 3860, pp. 115-131, Springer-Verlag, 2006

[vda5501] Verband der Automobilindustrie: VDA-5501 RFID im Behältermanagement der Supply-Chain, November 2006

[yu06] Y. Yu, Y. Yang, Y. Fan, H. Min: Security scheme for RFID tag, Auto-ID Labs Fudan University, White Paper, 2006

[vdc06] VDC: Pharma Item-Level RFID to Set Precedent, RFID Update, www.rfidupdate.com/articles/index.php?id=1222, October 2006

Authors

Thomas Hollstein

Dr.-Ing. Thomas Hollstein graduated from Darmstadt University of Technology in Electrical Engineering / Computer Engineering in 1991. In 1992 he joined the research group of the Microelectronic Systems Lab at Darmstadt University of Technology. He worked in several research projects in neural and fuzzy computing and industrial VHDL based design. Since 1995 he focused his research on hardware/software codesign and in 2000 he received his Ph.D. on “Design and interactive Hardware/Software Partitioning of complex heterogeneous Systems” at Darmstadt University of Technology. Since 2000 he is working as a senior researcher, leading a research group focusing System-on-Chip communication architectures and integrated SoC test and debug methodologies. He has been an initiator for a new research initiative in the field of printed electronics at TU Darmstadt starting in 2005 and is leading a research group for printed RFIDs since 2005. Since 2005 he is responsible for the ITG/VDE competence initiative "Fokusprojekt RFID" and he is the initiator and main responsible for the European Workshop "RFID Systems and Technologies" (RFID-SysTech).

Furthermore he is giving lectures on VLSI design and CAD methods. From 2001 until now he has been member of a leader team initiating and establishing a new international master programme in “Information & Communication Engineering” at Darmstadt University of Technology.

Manfred Glesner

Prof. Dr. Dr. h.c. mult. Manfred Glesner graduated from the Saarland University in Saarbrücken (Germany) in Applied Physics and Electrical Engineering in 1969. In 1975, he received the Ph.D. degree from the same university with research on the application of non-linear optimisation techniques in computer aided design of electronic circuits. From 1975 to 1981 he was a lecturer at the Saarland University in the areas of electronics CAD and control. In 1981 Manfred Glesner was appointed as an Associate Professor for electrical engineering at Darmstadt University of Technology, Germany. In 1989 Darmstadt University conferred him as a Full Professor the new chair of Microelectronics System Design. In 1996 and 1997 he received the honorary doctoral degree from Tallinn Technical University and the University of Bukarest. Since 2000 he is “Fellow of the IEEE”. Current research work is devoted to advanced design tools for microelectronic and nanoelectronic circuits, system integration on silicon, reconfigurable systems and VLSI architectures for mobile communication systems. He is a member of several technical societies and he is active in organizing international conferences.

Ulrich Waldmann

Ulrich Waldmann is a graduated chemist from the University of Freiburg and a graduate computer scientist from Darmstadt University of Technology. In 2002 he joined the working group "Smart devices and embedded security" at the Fraunhofer Institute for Secure Information Technology (SIT) in Darmstadt. His working fields are RFID, smart cards, standardization of smart card technology and biometrics, design and implementation of cryptographic protocols, specification of card applications for the German healthcard and health professional card. He was engaged in projects of card performance tests and development of secure card application systems, and has contributed to several technical reports in the fields of eHealth, card technologies and RFID. He is co-organizer of the annual SIT SmartCard Workshop.

Henk Birkholz

Dipl.-Inf. Henk Birkholz graduated from the Universität Bremen in Computer Science in 2006. Thereafter, he joined the Center for Computing Technologies (TZI) of the Universität Bremen. His work concentrated on security and scalability issues in Voice-over-IP networks. He worked on several research projects in cooperation with industrial partners and governmental agencies, specifically, with a strong focus on WLAN usability and security. In current research projects, he is responsible for the evaluation of management- and security-related implications in heterogeneous network environments.

Karsten Sohr

Dr. Karsten Sohr works at the Center for Computing Technologies (TZI) of the Universität Bremen, Germany. Prior to joining the TZI, he received his doctoral degree from the Universität Marburg, Germany, with a doctoral thesis on “Security Aspects of Mobile Code”. He is currently coordinator at the TZI for the research area security. His research interests include role-based access control, security of mobile applications and security engineering.