Data-on-Tag: An Approach to Privacy friendly Usage of RFID Technologies

Kerstin Werner[1], Eberhard Grummt[1,2], Stephan Groß[2], Ralf Ackermann[1]

[1] SAP Research CEC Dresden, 01187 Dresden, Germany
[2] Technische Universität Dresden, Institute for System Architecture, 01062 Dresden, Germany

Abstract

The proliferation of RFID technology in many application areas has caused serious concerns regarding threats to consumer privacy. To a large extent, this is due to the widespread approach of storing RFID-based data via a global network *(Data-on-Network)*, enabling its linkage and analysis. Based on a description of existing privacy threats and a presentation of the two general storage approaches, we argue that privacy concerns can be narrowed down by exclusively storing data on RFID tags *(Data-on-Tag)*. We support this assumption by presenting advantages for consumers as well as for companies and describe some novel application areas emerging from tag-centric approaches.

1 Introduction

The usage of RFID-based solutions already plays an important role in different application areas like production, supply chain management, healthcare, and finance. It allows to uniquely identify objects that are tagged with RFID transponders, enabling typical Auto-ID infrastructure services. Data transmission is done via a wireless radio wave link that also provides energy to the so called passive RFID tags. These respond to queries, sending information to RFID readers that are typically also responsible for performing initial data processing and forwarding to software systems for further usage.

One of the important decisions within an RFID scenario is where data should be persistently stored and accessed from. There is a general distinction between *Data-on-Tag* (DoT) and *Data-on-Network* (DoN), but also *hybrid* approaches combining both techniques exist. Nevertheless, at the moment solutions typically apply the DoN approach. In this case, only a unique identifier (ID) is stored on the tag. This ID is used as a link to more complex associated data that is stored in one or many networked backend systems. Standardization for this method has stepped forward comparably fast already, and has thus (in combination with only minimal requirements and resulting costs for the tags) caused widespread deployment and usage. The persistent storage of a huge amount of "rich" information in the network and the potential misuse resulting from its access, combination, and data mining has recently caused relevant concerns and even fear from end users who are afraid of insufficient data and privacy protection. These concerns result to a significant extent from the potential personalization of data and the extraction of profiles that are associated with individual persons [1, 2, 3].

In contrast to the above-mentioned DoN approach, all relevant information is stored on the tag in the DoT case. This method has gained less attention both within academic literature as well as for deployment so far.

We argue that the usage of DoT is a feasible method for reducing consumer fears concerning privacy aspects. The remainder of this paper is structured as follows: Section 2 presents the basics for DoT and DoN. Section 3 provides a general overview of potential privacy threats resulting from RFID usage. Based on this categorization, we discuss the benefits resulting from the usage of DoT and give indications for rating this approach as "privacy friendly" (Section 4). Furthermore we show promising usage and application potentials that result from storing additional information on tags. In Section 5 relevant drawbacks resulting from the utilization of DoT are discussed. Section 6 categorizes related work and shows correspondences to our approach. Finally, Section 7 summarizes our results and discusses potential future work.

2 Approaches to Data Management in RFID Applications

DoN and DoT are the two general ways of managing and distributing information within RFID systems. This section introduces and discusses their basic characteristics.

2.1 Data-on-Network

The DoN approach is illustrated in **Figure 1**. All additional data associated with a specific unique ID is stored either centrally or distributed within a network. This procedure exactly corresponds to the ideas described within the EPCglobal [4] standardization framework. This framework is the outcome of a joint effort for standardizing RFID usage within logistic applications and has lead to a number of documents and procedures that are already commonly agreed about.

One of the benefits of this approach results from the limited requirements concerning tag capacity and features. The possibility to use WORM (Write Once Read Multiple) tags

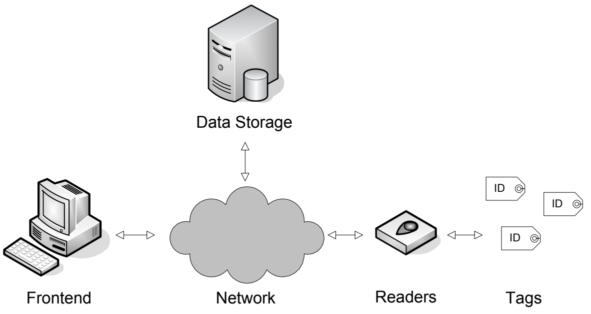


Figure 1 Data-on-Network: General architecture

allows for both flexibility as well as lowered costs. Another advantage is the opportunity to easily track and trace tagged objects. This is especially important for companies cooperating in supply chains because it enables them to proactively operate and to trace back the complete history of specific objects.

In contrast to the benefits we have listed, there is a dependency from the availability and proper function of the necessary network connectivity and storage systems. On the other hand, information about tagged items is obtainable even if the item itself is temporarily unavailable or generally lost. Therefore, DoN is especially favorable if multiple or concurrent access operations from different participants have to be supported and persistent availability of item information is needed.

2.2 Data-on-Tag

Utilizing the DoT approach (see **Figure 2**), all relevant data that is associated with a specific object is stored in addition to an ID on the tag itself. This way, all information about an object can be immediately obtained even if there is no network access available. The object itself might carry all the information about its identity, state, quality characteristics, history, and its designated future with it.

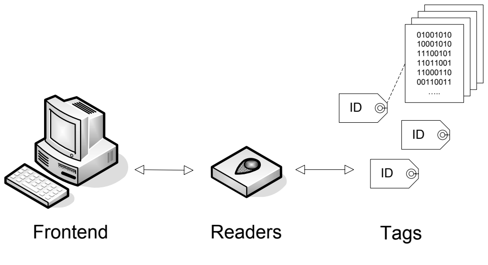


Figure 2 Data-on-Tag: General architecture

Due to the potential spatial distribution of objects and data this approach is often called decentralized data management. There is no need for a specific network infrastructure to access data related to an object. These characteristics are especially favorable for applications that depend on the availability of object-related information but can't ensure a reliable network connection. In case a larger amount of data has to be stored there are some implications to take care of. These comprise the amount of available storage, appropriate formats and the time for data transmission. Besides, stored data typically needs to be written and changed over time. Efforts for standardizing storage as well as encoding schemes play an important role. They are due to the extended amount of information and its application dependency not generally agreed upon so far.

3 Privacy in RFID Systems

This section describes privacy concerns arising from the deployment of RFID systems and existing approaches to their reduction.

Privacy aims to protect persons against misuse of individual-related data. By retrieving data from RFID tags using RFID readers, information of two different types can be accumulated:

Content contains anything from unambiguous IDs up to any other kind of imaginable information that can be stored on the available tag memory. Usually, this information directly refers to some of the tagged object's properties.

Context may include any kind of static or sensor-based data such as the time of read events and properties of readers like their identifier or position. Anybody in control over a reader might be able to harvest this information by reading out surrounding tags. That way it is furthermore possible to observe and track people's movements as long as they are associated with the possession of one ore more certain tags ("*constellations*"). This clearly endangers privacy rights of people carrying RFID tags or tagged objects.

Using the DoN approach, content and context data will be permanently stored and exposed to legitimate users via a network (while also being prone to attacks by adversaries). Based thereon, it is possible to merge available datasets, to analyze and join them with data from external sources or to share them with others. Collected data can be easily associated with certain people because the contemplable subgroup can be extremely narrowed down that way. This enables the creation of individual-related profiles of many different kinds.

Concerning privacy threats in RFID systems, it is often distinguished between threats to *data privacy* (aiming at content) and threats to *location privacy* (aiming at context) [5]. Threats to data privacy emerge from personalization, linkage, evaluation and dissemination of content data. This way, it is possible to discover social networks, to create customer profiles but also to spread false information about specific persons.

On the other hand, threats to location privacy comprise the collection of data that provides information about where a certain person is or has been. By tracking persons and maybe even joining the resulting location data with datasets of external sources, movement profiles can be derived. The higher the distribution of RFID readers, the easier it will be to track movements of RFID tags. **Figure 3** represents the discussed coherences.

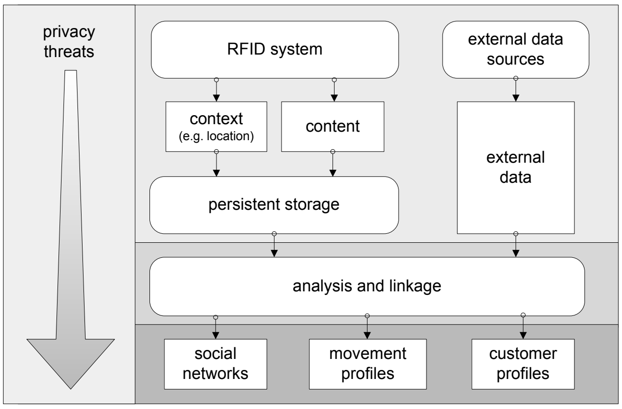


Figure 3 Threats to privacy occuring from the collection and processing of RFID-based data

Due to several technology specific features, the named privacy threats are especially critical in RFID systems. For example bulk reading facilitates the efficient, almost simultaneous readout of a large amount of RFID tags. The possibility to gather data from a distance and without intervisibility of tags and readers enables unnoticed readouts. Furthermore, the provision of RFID-based data in a global network is strongly promoted by recent efforts in standardization for the DoN approach.

These threats to consumers demand the compliance with specific requirements on the part of companies that apply RFID technology [6, 7]. These can be summarized as follows:

Transparency: Usage, intended purpose and stored data on tags, which are applied to products in the possession of consumers, have to be easily for them to pursue.

Notification: The unnoticeable utilization of the technology and especially the unnoticeable communication between tags and readers has to be hindered.

Opt-In: The agreement of the involved subject is an indispensable prerequisite for the collection of individual-related data and the linkage with other data sources.

Limitation to specified purpose: Collection and usage of RFID-based data has to be limited to the purpose specified and declared to consumers beforehand.

Appropriate security measures: It has to be ensured that appropriate measures of data protection regarding confidentiality, integrity and availability of accumulated data are applied.

No creation of individual-related profiles: Data has to be stored and processed separately relating to specific products, to prevent the extraction of consumer profiles e.g. regarding their movements, interests and social relationships.

Blocking mechanisms: Any possibility of undesired readouts of tags on the part of consumers has to be eliminated.

Deactivation mechanisms: Consumers must have the opportunity to deactivate RFID tags on their products or delete stored data after purchase without experiencing any discrimination.

Unfortunately, the development and deployment of privacy protecting guidelines and technical measures in the field of the RFID technology is not solely driven by consumers but also by companies that produce, sell and apply the technology to gain benefits. These companies do not want to be restricted by any rigid regulations, but rather want to take full advantage of RFID. That's why most of them argue that the collection, storage and processing of RFID-based data is already appropriately supported by currently existing laws. On the other hand, they are aware of the fact that the utilization of the technology has to be accepted by consumers to unfold its full potentials [8, 9].

It is obvious that it has to be agreed upon a trade-off between both the consumers' and the companies' points of view to make successful use of the technology. Possible solutions that could address these multilateral requirements include legal restrictions, voluntary commitment certification mechanisms or the application of appropriate technical, organizational or physical measures [10].

The consumers' requirements regarding the utilization of the RFID technology named above are currently addressed by legal restrictions which differ from country to country. In Germany, legal restrictions concerning privacy exist on both federal and federal state level. These are influenced by the privacy guidelines passed by the EU in 1995 that are intended to be implemented by all Member States. These guidelines implement in turn the Fair Information Practices (*FIP*) passed by the OECD in 1980. The FIP are intended to guarantee a minimum protection regarding collection and processing of data. Besides these legal restrictions, several technical approaches which are supposed to enforce privacy in RFID systems exist. In [5, 6, 11], various solutions to privacy and security protection are introduced. Furthermore, [12] precisely examines how the FIP could be realized in RFID solutions.

Our approach integrates itself into technical solutions by proposing that several privacy threats could be constrained just by storing data exclusively on tags. In the following section we give reasons that support this approach and describe it in more detail.

4 Potential Benefits of Data-on-Tag

In this section, we argue that the DoT approach promises to enable strong privacy protection while still providing useful additional functionality to the consumer.

4.1 Avoiding Centralized Storage, Linkage and Analysis

As described in Section 1, the deployment of DoN prevails compared to DoT. As shown in the previous section, several privacy threats arise from the persistent storage on the network in combination with further processing. By solely storing such information directly on the respective transponders, corresponding data on the network is not existent and thus can not be abused. A global view of transponder-related information can not be generated simply because the necessary data is, along with the tags, physically distributed and thus not directly accessible.

4.2 Improved Control by Consumers

By storing data on tags, consumers can be given additional control over the respective information, supporting their informational self-determination. As long as tags are clearly identifiable as such and detachable from products, they can be physically destroyed by users. Provided that an appropriate technical infrastructure is available, they can also read, edit and delete their content. From a certain point of view, such tags are comparable to Cookies in Internet Browsers. Cookies are small files storing personal, custom information at the client's PC. This information can be accessed by the issuing web site, but can also be viewed, deleted or modified by users - even though appropriate editors are not built into current browsers.

Given adequate RFID tags, users could also define who can read or write which data. This can be realized in different levels of detail, from using a simple write protection bit to employing a fine-grained access control system. However, the latter approach introduces challenges regarding usability, identification and authentication of participants as well as key distribution.

4.3 Increased Consumer Acceptance by Providing Additional Value

Companies sometimes try to increase consumer acceptance of new technologies by providing adopters additional value, e.g. new functionality. For example, domestic appliances could determine which products they contain by means of RFID tags, enabling them to provide consumers with relevant information such as recipes, expiry dates, and the like. The DoN approach to such services would introduce the question how consumers can access the relevant information on the network. Managing access rights as well as the infrastructural connection to the relevant data sources pose technical and financial challenges.

In the case of rewritable tags, DoT can also enable users to customize their object's digital properties. This can both support privacy [13] and provide additional functionality. A user could assign a chosen ID or personally meaningful, identifying or describing information to a tag. External stakeholders would be impaired in their ability to make sense of this data because of the lack of uniquely identifying patterns.

Consumers could assign self-chosen keywords to their tagged objects (virtually "tagging their tags") to enable improved recognition, sorting, and grouping of their belongings.

4.4 Benefits for Companies

Enterprises can benefit from DoT approaches, too. Companies that frequently change their partners (e.g. suppliers) can profit from tag-based data exchange by saving costs involved in establishing and maintaining network infrastructures. Mobile RFID readers could be lent to current partners and taken away after the cooperation is over, leading to improved protection of investment. If network access is not available in the first place, for example at offsite production plants, DoT might be imperative to enable certain application at all. Complex access control mechanisms for background systems become dispensable, as access rights are directly inferred by the physical access to the tagged object. In the future, rewritable tags promise to empower self-controlling logistic networks. "Smart containers" might autonomously find their destination or, in combination with sensors, collect context information as they travel through the supply chain. Moreover, "Digital packing slips" could enable object-related, asynchronous message exchange between multiple partners. Future RFID tags featuring enhanced computational power and field programming capabilities might very well enable highly scalable, dynamically distributed systems. By distributing computation and storage tasks among the tags, dependability on bottlenecks such as central databases or permanent network connections can be limited. Several B2B and B2C applications of RFID tags turned Smart Items can be envisioned based on insights from sensor network research.

4.5 Anti Counterfeiting and Supply Chain Integrity Monitoring

Using RFID-based technology to prevent or detect counterfeiting of high-value goods and pharmaceuticals currently forms an active field of research. There are two main ideas to enable detection of bogus products equipped with RFID tags. Either a genuine tag attached to the item is designed to be technically hard for the attacker to clone (similar to holograms). Or the detection of counterfeit products is based on the pedigree that is linked to it via its tag's ID.

Being able to tell whether a product is genuine or forged can be advantageous for consumers in that they don't purchase inferior quality or potentially dangerous goods. Of course, companies strive for making counterfeiting their products as hard as possible while also considering costs of the countermeasures to limit their losses.

The DoT approach may introduce enhanced functionality such as tamper evidence and stored pedigree records. Tamper evidence can be achieved by using active tags in combination with sensors. For example, goods can be marked as spoiled when a temperature sensor has detected that the cool chain has been interrupted too long. A product's pedigree can be stored on the respective tag, consisting of electronically signed entries by all supply chain partners. Even their test keys can be stored on the tag, although these ultimately would need to be verified by a trusted authority.

5 Discussion

In Section 4 we provided several potentials of DoT that could be of use for consumers but also for companies. Facing these, we now discuss potential drawbacks and consequences of this approach.

5.1 Restricted Tracking and Tracing

The most serious disadvantage of not storing tag-related read events in databases is the disability to easily track and trace items. Given enough memory and advanced authenticity measures, one could save an item's tracking history on its tag. But this would still conflict with the vision of the "Internet of Things" in which the digital representation of a physical object is available from anywhere in the world using the Internet. This is also the most dominant criticism of the pure DoT approach.

One could conclude that DoN enables cheap solutions and convenient surveillance of items (and thus their holders), while DoT promises more privacy friendly solutions, sacrificing several features desired mainly by the industry. Hybrid solutions may bring together the best of both worlds. It is however unclear how this can be achieved in detail. Tracking and tracing, and thus violations of consumers' location privacy, will be possible once data linked to a tag via a unique ID is stored on a network. So one question is how these unique IDs can be avoided, while still enabling the respective applications and also handing over some control to the final consumer, which is not known beforehand.

We argue that "hybrid" can mean two different things. Firstly, a hybrid RFID tag can store information in its internal memory and can also be linked to information in external databases via a unique ID. This is the most common definition of hybrid RFID tags. Secondly, a tag could change its behavior once it has been handed over to the consumer, basically turning it into a "private" tag disabling further tracking and enabling useful personal functionality.

We also believe that the distinction of DoN and DoT is just a first and very coarse-grained step to classifying RFID tags at a functional level. Privacy friendly RFID usage is not only concerned about what information is stored where and how it can be linked and by whom, but also how especially the consumer can be involved in these decisions.

5.2 Advanced Requirements

Many of the outlined applications of the DoT approach involve advanced requirements, both regarding hardware and software as well as user acceptance and education. Clearly, RFID tags providing sufficient amounts of read-write memory, sensors, and access control facilities have an impact on both price and development and deployment efforts. Consumers would have to be equipped with devices enabling control over a tag's content and access control rights, so prerequisites include social acceptance, ease-of-use, and substantial incentives to foster respective purchase decisions.

Especially the management of access rights and corresponding keys ("who is allowed to read or write which region of a given tag?") poses a serious challenge. Users want to grant or deny access to different companies. The tag should then, on their behalf, verify if an attempted access is legitimate or not, which includes checking if the respective company is who it claims to be. To do so, it must have access to the (trusted) test keys of the company in question, or at least to the test keys of trusted certification authorities. Implementing these mechanisms given the restrictions imposed by tags constitutes a challenging task.

5.3 Increased Costs

Using DoT, the required tag memory capacity is larger than in comparable DoN scenarios. Simple WORM tags are usually not sufficient, since data on the tags has to be modified and updated during the tag's lifecycle, so RW (read/write) tags are necessary. Exclusively storing information on the tags also shifts data security threats, especially regarding confidentiality of contents, to the tag level and the air interface, which need to be carefully protected, both physically and logically. Encryption, access control, and key management facilities lead to more complex and expensive chip designs. However, the ongoing trend towards cheaper and more powerful computing devices also applies in the radio frequency domain, so that advantages of sophisticated DoT solutions may soon outweigh the involved investments. Moreover, tags could be reused multiple times.

5.4 Few Efforts in Standardization

Current efforts in standardization of RFID applications are mainly focusing on the DoN approach. This facilitates the production and sales of RFID tags that suit the associated requirements. The main problem with standardizations that could support the DoT approach is that data stored on tags strongly varies depending on specific industries, applications, and contexts such as different trust relationships or technical conditions. DoT is not as much established as DoN yet. However, this trend could be altered by paying more attention to DoT and examining its full potentials in research and industry in more detail. Increased standardization efforts in the DoT approach would even positively influence the relatively high costs for tags mentioned earlier in this section and foster its adoption.

6 Related Work

Diekmann et al. give an overview of the two approaches DoT and DoN focusing on economic aspects. They support our approach by promoting the potentials of DoT and hybrid solutions and by stating that they have gained insufficient attention so far [14].

Floerkemeier et al. discuss several threats to privacy in RFID systems. To address these, some technical solutions are proposed which especially aim to assert compliance with the FIP [12].

Contributions of Garfinkel [6, 11] deal with privacy threats as well as security risks caused by the deployment of RFID solutions. Their main focus is on the consideration of demands of different stakeholders as well as the examination of related wireless technologies.

Rieback et al. relate to our approach by introducing a platform that is intended to improve consumer's control over their data and thus enabling privacy and security in RFID systems. The platform called "RFID Guardian" resembles an "RFID firewall" which provides access control mechanisms to secure contents stored on tags but also raises questions regarding usability [15].

7 Summary and Future Work

This paper described the two approaches DoN and DoT and gave an introduction to potential privacy threats in current RFID systems, including threats to consumers' location privacy and data privacy. We stated that these mainly result from the deployment of DoN because this approach enables rapid undesired linkage, evaluation and sharing of collected data. We proposed that many of these threats can be mitigated utilizing the DoT approach. Therefore, we stated several advantages and potentials of DoT supporting our suggestion, including benefits to both consumers and companies. The approach especially respects important RFID-specific consumer requirements regarding privacy listed in Section 3. This supports our opinion that DoT, combined with other technical measures and legal restrictions, is a promising solution to provide consumer and privacy friendly deployment of RFID technology. It also holds a great potential for new application areas.

Our statements are based on the assumption that applying the DoT approach means that data is exclusively stored on tags and is really not stored or made available over a network. Therefore, they are partially based on trust in system providers. Facing this, it is interesting to analyze how these assumptions can be technically enforced.

In Section 4.2, we showed that the usage of DoT enables end users to keep control over their data. This infers that they have to be sensitized and provided with appropriate equipment. In our future work, we want to evaluate how such equipment can be designed and how flexibility and security need to be traded off against usability, as consumer acceptance is imperative for such equipment's success. Especially, we want to explore how tag awareness can be improved, how effortless user interactions can be designed, and how personal information on tags can be managed. Using Bluetooth enabled RFID readers, we want to connect mobile phones and PDAs equipped with our prototypical software to demonstrate the developed concepts.

While utilization of DoT-based systems generally limits the possibilities of analysis and linkage of RFID-based data, misuse by unauthorized reading and writing of tags might still be feasible. This raises questions regarding the deployment of adequate access control mechanisms on the level of RFID tags.

The DoT approach demands the use of rewritable tags in many application scenarios. This requires the strengthening and adaptation of existing input controls and filtering on reader and middleware levels because rewritable tags might be used to infiltrate malware into systems [16]. However, considering complex reprogrammable tags, infection is also possible in the other direction, something that needs to be considered in scenarios where untrustworthy parties are granted write access to tags.

Regarding an in-depth security analysis, other possible attacks should be considered as well, using lessons learned from related technologies such as smart cards and payment systems. Small tokens given to consumers can always be compromised. This needs to be kept in mind when designing systems based on such tokens, for example by considering all input data as potentially untrustworthy and by reducing the attacker's incentives for manipulation.

8 References

[1] GÜNTHER, Oliver ; SPIEKERMANN, Sarah: RFID and the perception of control: the consumer's view. In: *Commun. ACM* 48 (2005), Nr. 9, S. 73–76. – ISSN 0001–0782

[2] ECKFELDT, Bruce: What does RFID do for the consumer? In: *Commun. ACM* 48 (2005), Nr. 9, S. 77–79. – ISSN 0001–0782

[3] LANGHEINRICH, Marc: Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie. In: FLEISCH, Elgar (Hrsg.) ; MATTERN, Friedemann (Hrsg.): *Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis.* Springer-Verlag, 2005, S. 329–362

[4] TRAUB, Ken ; ALLGAIR, Greg ; BARTHEL, Henri ; BURSTEIN, Leo ; GARRETT, John ; HOGAN, Bernie ; RODRIGUES, Bryan ; SARMA, Sanjay ; SCHMIDT, Johannes ; SCHRAMEK, Chuck ; STEWART, Roger ; SUEN, KK. *The EPCglobal Architecture Framework – EPCglobal Final Version of 1 July 2005.* http://www.epcglobalinc.org/standards/Final-epcglobal-arch-20050701.pdf. July 2005

[5] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK. *Risiken und Chancen des Einsatzes von RFID-Systemen (RIKCHA) - Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit.* http://www.bsi.bund.de/fachthem/rfid/RIKCHA.pdf. 2005

[6] GARFINKEL, Simson ; ROSENBERG, Beth: *Garfinkel, S: RFID. Applications, Security, and Privacy.* Addison-Wesley Longman, Amsterdam, 2005. – ISBN 0321290968

[7] KERN, Christian: *Anwendung von RFID-Systemen (VDI-Buch).* Springer, Berlin, 2006. – ISBN 3540444777

[8] THIESSE, Frédéric: Die Wahrnehmung von RFID als Risiko für die informationelle Selbstbestimmung. In: FLEISCH, Elgar (Hrsg.) ; MATTERN, Friedemann (Hrsg.): *Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis.* Springer-Verlag, 2005, S. 363–378

[9] HANDY, Matthias ; TIMMERMANN, Dirk: Kleine Chips mit großer Wirkung - Über die Akzeptanzprobleme der RFID-Technologie. In: *Workshop*

zu Sozialen Implikationen von Ubiquitous Computing Technologien, 2004

[10] GABRIEL, Peter. *RFID in der Logistik - Chancen für den Standort Deutschland.* VDI/VDE Innovation + Technik GmbH. January 2005

[11] GARFINKEL, Simson ; JUELS, Ari ; PAPPU, Ravi: RFID Privacy: An Overview of Problems and Proposed Solutions. In: *IEEE Security and Privacy* 3 (2005), May-June, Nr. 3, S. 34–43

[12] FLOERKEMEIER, Christian ; SCHNEIDER, Roland ; LANGHEINRICH, Marc: Scanning with a Purpose – Supporting the Fair Information Principles in RFID protocols. In: MURAKAMI, Hitomi (Hrsg.) ; NAKASHIMA, Hideyuki (Hrsg.) ; TOKUDA, Hideyuki (Hrsg.) ; YASUMURA, Michiaki (Hrsg.): *Ubiquitious Computing Systems. Revised Selected Papers from the 2nd International Symposium on Ubiquitous Computing Systems (UCS 2004), November 8-9, 2004, Tokyo, Japan* Bd. 3598. Berlin, Germany : Springer-Verlag, Juni 2005. – ISBN 3–540–27893–1, S. 214–231

[13] INOUE, Sozo ; YASUURA, Hiroto. *RFID privacy using user-controllable uniqueness.* RFID Privacy Workshop, MIT. 2003

[14] DIEKMANN, Thomas ; MELSKI, Adam ; SCHUMANN, Matthias: Data-on-Network vs. Data-on-Tag: Managing Data in Complex RFID Environments. In: *hicss* 0 (2007), S. 224a. – ISSN 1530–1605

[15] RIEBACK, Melanie ; GAYDADJIEV, Georgi ; CRISPO, Bruno ; HOFMAN, Rutger ; TANENBAUM, Andrew: A Platform for RFID Security and Privacy Administration. In: *Proc. USENIX/SAGE Large Installation System Administration conference.* Washington DC, USA, December 2006, S. 89–102

[16] RIEBACK, Melanie R. ; SIMPSON, Patrick N. D. ; CRISPO, Bruno ; TANENBAUM, Andrew S.: RFID Malware: Design Principles and Examples. In: *Pervasive and Mobile Computing (PMC) Journal* 2 (2006), S. 405–426

Kerstin Werner
SAP Research CEC Dresden
T: +49 (351) 481 161 34 F: +49 (6227) 784 691 2 E: kerstin.werner@sap.com

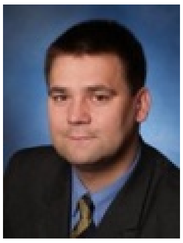
Kerstin Werner joined SAP Research CEC Dresden in 2006 as a student employee. She became a Research Associate in SAP Research's PhD program after finishing her diploma thesis. Her interests in research include RFID usage in cross-enterprise scenarios, resulting problems concerning security, privacy and trust and Service Description Languages, particularly methods of describing non-functional properties like quality and trust.

Eberhard Grummt
SAP Research CEC Dresden
TU Dresden, Chair for Computer Networks
T: +49 (351) 481 161 33 F: +49 (6227) 784 752 1 E: eberhard.oliver.grummt@sap.com

Eberhard Grummt joined SAP Research and the Chair for Computer Networks at the Technische Universität Dresden as a Research Associate in 2006. His research interests comprise distributed, multilateral access control and credential management in Auto-ID based enterprise applications as well as distribution and coordination aspects of distributed systems.

Stephan Groß
TU Dresden, Chair for Computer Networks
T: +49 (351) 463 382 13 F: +49 (351) 463 382 51 E: stephan.gross@tu-dresden.de

Stephan Groß joined the Chair for Computer Networks at the Technische Universität Dresden in 2003. Prior to his current position, he worked as a researcher and consultant at the Fraunhofer Institute for Experimental Software Engineering. His research interests are related to security in networked environments, especially multilateral secure distributed systems, distributed trust management and practical implications of IT security.



Dr. Ralf Ackermann
SAP Research CEC Dresden
T: +49 (351) 481 161 32 F: +49 (6227) 784 746 8 E: ralf.ackermann@sap.com

Ralf Ackermann joined SAP Research Dresden in July 2006 as a Senior Researcher. He holds a diploma and a doctoral degree in Computer Science. His research interests are (context-controlled) advanced IP communication and IP telephony, ubiquitous communication and computing, embedded and wearable systems, RFID systems, sensor networks as well as network and system security and privacy.