RFID Data Management in Supply Chains: Challenges, Approaches and Further Research Requirements

Adam Melski, Lars Thoroe and Matthias Schumann

University of Goettingen, Institute of Information Systems, Dep. 2, Goettingen, Germany

Abstract. The implementation of RFID leads to improved visibility in supply chains. However, as a consequence of the increased data collection and enhanced data granularity, supply chain participants have to deal with new data management challenges. In this paper, we give an overview of the current challenges and solution proposals in the area of data collection and transformation, data organization and data security. We also identify further research requirements.

1 Introduction

As a result of, in particular, efforts towards standardization and the falling costs of technology, RFID (Radio Frequency Identification) systems are leaving their niche and are being increasingly implemented in an effort to eliminate inefficiency and the lack of visibility in global supply chains. Large retailers like Wal-Mart [1] and Metro [2] function as the primary pioneers in the introduction of RFID, but smaller businesses, for instance, the medium-sized textile company Lemmi Fashion [3], have recently started to optimize their supply chains with the help of this new technology as well. Above all, the implementation of RFID leads to improved visibility in complex and, when using conventional technologies like the barcode, hardly transparent, supply chains [4]. These advantages are being utilized in at the expense of new challenges in the area of data management, which can be primarily attributed to the rise in data volumes. The substantial data volumes are a result of the increased amount of data capture points, more frequent capture sessions and enhanced data granularity. Considering this background information, the following areas of investigation can be identified:

- *Data capture and transformation:* RFID systems function first and foremost as data generators. Because of the physical characteristics of the technology, the data are often faulty (dirty data). Besides, the data possess a raw character (low-level data) and must therefore be filtered from the middleware, compressed and properly transformed before being relayed to their respective application systems (high-level information).

- *Data organization:* The exchange of object related data has seen a significant increase in RFID-supported supply chains. The provision and relay of the data

Melski A., Thoroe L. and Schumann M. (2007).
RFID Data Management in Supply Chains: Challenges, Approaches and Further Research Requirements.
In *Proceedings of the 1st International Workshop on RFID Technology - Concepts, Applications, Challenges*, pages 61-74
DOI: 10.5220/0002413200610074

represent new challenges for the hitherto existing informational architecture in business networks.

- *Data security:* The more data on their products businesses save and exchange, the simpler it becomes for competitors to gain access to these data. These businesses are therefore exposed to a greater danger of manipulation and unauthorized data retrieval, particularly because of the fact that data are stored directly on the object.

This contribution provides an overview of the current challenges and solution proposals in the above-mentioned areas of data management in RFID-based supply chains. Besides the illustration of the present state of research, the demands of future research will be identified. In section 2, general data management challenges will be derived based on the characteristics of RFID systems. Thereupon, current data management concepts will be presented in section 3 on the basis of the three identified areas of data management. Furthermore, future research questions will be identified in this section. Finally, section 4 concludes with a short summary.

2 RFID Data Management Challenges

RFID systems use radio waves to facilitate communication between transponders and readers. This leads, on the one hand, to the capability to identify objects from a reasonable distance without line of sight; on the other hand, the identification process is subject to conventional physical influences and can lead to reading anomalies (e.g. tags are not recognized). Besides, mistakes can occur at the operational process level. For example, a product in the supermarket can make its way more than once from the warehouse to the supermarket shelf and back again (e.g. because there's no shelf room). Such cyclic object movements could be interpreted as anomalies and then wrongly filtered by the system [5]. Besides, if sensors which, for instance, measure the local temperature are implemented in addition to RFID tags, then they can cause incorrect data to be delivered because of a technical defect [6]. For the reasons just named, the demand for increased data filtering in RFID systems is collectively posited in the relevant literature [7] [8] [9].

Data capture by means of RFID requires no manual actions, which causes a decrease in the cost of the data capture process. This implies that the number of capture sessions and points increases. For instance, with the implementation of so-called smart shelves, data from the objects on the shelves can be read continuously. This has multiple effects:

- Firstly, the data quantity increases significantly. These data must be compressed before they are relayed. On this point, the implementation of so-called aggregation methods is discussed in the literature [10]. These methods decrease data quantity without loss of information. In addition, suitable archiving methods should be implemented as a means of separating old, as well as obsolete, data from data being presently used. This would guarantee a better system performance [11]. This is because, in RFID systems, which, above all else, create a memory map of the real world in its digital counterpart, current data (e.g. concerning ongoing good movements) are of primary interest [12].

- Secondly, RFID data are quite dynamic, whereby the time component must be adequately mapped. New data models are therefore necessary [13].
- Thirdly, the data accumulate continuously (asynchronous) [14]. Whereas a barcode is only read when needed, transponders continually transmit data to the reader. These data must be processed in real-time and then relayed to the connected systems.
- Fourthly, as objects pass multiple read points, data from different readers must be compressed to complex events which represent the object flow. This generally occurs through the definition of predefined rules [15].

RFID allows the data from multiple objects to be read simultaneously (bulk reading). Possible collisions, by which more than one signal arrives simultaneously, and therefore cannot be separated by the reader, must be avoided through the implementation of anti-collision algorithms [16].

The efficient identification procedure of RFID is not the only reason why it is of interest for business processes. Rather, it is the ability to store data directly on the object that provides impetus for innovative implementation. The fact that the data are bound to the object means that they can be read at all times by whoever is the temporary possessor of the object. Although this, in most cases, is not problematic, being even desired, there are certain 'sensitive' data which should not be accessible to everyone. This is, as a result of public discussion, especially the case as it pertains to consumer privacy (for instance, pertaining to shopping at the supermarket) [17]. But companies also cannot afford to give away sensitive data (e.g. product features, maintenance data). The data stored on the tag must therefore be adequately protected against potential abuse or manipulation. Suitable data protection mechanisms (e.g. encryption) must be implemented.

In open-loop supply chain applications, by which the tagged object runs through a series of supply chain levels, data stored on the object and/or in central databases should be accessible to all partners. Only in this way can the transparency in the supply chain be enhanced. The construction of an information network which spans all companies and makes access to these data possible is, consequently, necessary to this end. Furthermore, questions of data allocation and distribution (centralized/decentralized data storage) need to be considered.

3 RFID Data Management Concepts

3.1 Data Collection and Transformation

An important question in the area of RFID data collection in supply chains regards the data capture points and the tagging level (pallet/case/item). The vision of complete visibility through the use of RFID appears to be economically unreasonable in most cases. The relevant literature attests retail in particular as the last element in the supply chain high potential benefits through RFID data collection. Thus, the distribution of costs and benefits of an RFID implementation within supply chains continues to be an object of research [18] [19].

A further important area of research is the performance capability of the reading infrastructure. Two main factors are relevant for the measurement of the performance capability of a data capture system: accuracy and efficiency [20].

Acurracy: A 100% data capture is not necessary in all applications; however, in many cases – for instance, when striving to monitor product movement in supply chains exactly – a read rate of near to 100% is practically required. This rate, however, is often not achieved and faulty readings occur. The most significant example of faulty reading is the failure to identify tags which are located within the vicinity of a reader. The most important sources of these failures can be assigned to collisions [21] [22].

In order to avoid disturbances through collisions, there exist various anti-collision protocols; the development of effective and efficient algorithms remains, however, a topic of research [23] [24] [25] [26]. Another source of failures is the tag detuning, misalignment and shielding [21] [27].

A possible solution for this category of problems lies in the redundant implementation of RFID infrastructure. On the one hand, the accuracy of the system can be improved through the implementation of several readers with overlapping reader fields. On the other hand, several tags (so-called mirror tags) can be used for the identification of a single object [20].

Efficiency of data capture: An essential criterion in this case is the speed at which the tags are read. The speed at which a single tag is read depends on the frequency being used by the system as well as on the extent of the content to be read. The latter is greatly determined by the chosen form of data organization. The demand for research exists with respect to the question as to with which level of data organization the required speed of data provision for controlling the application can be reached. The quick bulk reading of several tags is equally a topic of current research [23].

For the afore-mentioned reasons, data input verification in RFID systems needs too be more sophisticated. Faulty readings have to be identified and eliminated. Several statistical techniques for the cleaning of RFID data are discussed in the relevant literature [5] [28] [29]. For instance, Jeffrey, Garofalakis, Franklin present an adaptive smoothing filter which aggregates and analyses the data from several read cycles using different, self-tuning window sizes [29].

Following the collection phase, the large quantities of raw data must then be transformed into usable information. The process of data transformation consists of the following steps: reduction of the quantity of data, selection of relevant data and generation of information which serves as a basis for decision-making.

The first two steps are generally taken over by the readers (intra-reader reasoning) [10]. The generation of information relevant to the decision-making process is, however, carried out by the connected middleware. This results from the fact that data from the local reader are no longer sufficient for this process, the generation of complex events requires an analysis of the data from multiple readers (inter-reader reasoning) [14].

Reduction of data quantity. In general, readers should only relay data to the middleware when additional information can be generated through the use of these data. For instance, if transponders are located within the reader field of a particular reader for a longer period of time, then the same data are read over and over again. For any particular user, however, the most important data are, first and foremost, those data pertaining to when the object entered the reading field of the reader and when the object moved outside the range of that reader. All readings that occur between these two events are redundant, because they deliver no new information on the status of the object. This implies that readings should only be relayed when the status of the object changes. In this way, the quantity of data is reduced without loss of information [8].

Selection of relevant data. In the next step, the pre-filtered data are subjected to a selection process. The following scheme, for example, can be used [8] [10] [30]:

- Combination: If a pallet, together with the objects that it contains, is identified, then these data can be combined into a cluster and relayed together.
- Passing process: If objects pass a gate (for instance, upon entering the warehouse), then, instead of the events 'object appeared' and 'object disappeared', only a 'pass event' should be relayed to the applications.
- Simplification of movement paths: For specific data analysis purposes, less important object movements (like the movement of an object from one warehouse shelf to another) can be simplified, without the loss of significant information.

Generation of information relevant to the decision-making process. In the final step of the transformation, information relevant to the decision-making process is generated from the already-filtered data. During this process, single events are aggregated to complex events [31], and RFID data are combined with additional context data, as well as being evaluated according to predefined rules [8]. If, for instance, a product was identified at specific read points, e.g. 'shelf' and then 'exit', without having first been identified at the read point 'cashier', then it could be a matter of theft.

Wang and Liu propose a new data model called DRERM (Dynamic Relationship ER Model) to adequately map RFID data in information systems [11]. Due to the addition of dynamic relations, the suggested model supports complex queries in the category of object monitoring and object traceability. Gonzales et al. introduce so-called RFID-cuboids, which represent RFID data on different abstraction levels (e.g. data is clustered and presented in an abstract way for decision-makers) [30].

3.2 Data Organization

There are two basic possibilities for data storage in RFID systems: Object-related data can be deposited in databases and referenced by means of a unique ID (data-on-network), or data can be stored on the transponder and therefore directly on the object (data-on-tag) [32].

Data-on-Network. In a data-on-network system, a unique ID is stored on the transponder while all other object related data remain in central databases, which can be either managed by an information intermediary or can maintain with the supply chain partners. This is mainly due to the fact that RFID was still too expensive at the end of the '90s for wide-scale implementation. RFID found itself in a vicious circle, in which high costs entailed a minimal adoption of the technology and a minimal adoption of the technology resulted in high costs. For this reason, low-cost transponders, simple data exchange protocols and elementary data structures were expected to lead to a breakthrough [33].

If an object is located within the reader field of an RFID reader, then a data quadruplet is transmitted, consisting of the reader ID, the antenna ID, the object ID and the time stamp of the reading [8]. With this information, it can be unequivocally determined where an object is/was located at what time. Further data can be retrieved, when needed, by the middleware over various networks (e.g. over the internet). In this case, the data source must be known, that is, the middleware must have access to information as to which database must be queried in order to retrieve the pertinent object data.

There are two conceivable possibilities for data storage in this case. On the one hand, object-related data can be stored centrally and administered by an intermediary; on the other hand, these data can be stored in each partners' local databases.

Case study: Forestry. In order to reduce the shrinkage rate of wood on its way from the forest to the saw mill, the leading German forestry company Cambium has been using RFID technology since 2005 [34]. The traditional process of putting a small plastic flag on the logs and then recording the relevant data on paper lead to 15 % shrinkage in quantity and quality. Therefore, the logs are now furnished with a nail-shaped RFID tag. The only information on each transponder is a simple unique ID. Further data (type of tree, length, quality etc.) are sent to a central database using a handheld device. The data are accessible to all participants in the supply chain (primarily the forest proprietor, forest workers, haulers, shippers and saw mills). In order to determine possible discrepancies in quantity, the tags are queried before each step in the transportation process and the relevant IDs are then transmitted to the central database. According to the company's initial calculations, it is assumed that the implementation of RFID will result in a 70 % reduction in shrinkage.

The case-in-point example of data organization using RFID technology distinguishes itself through the following advantages:

- From the perspective of the participants in the supply chain, it is a matter of a relatively simple organizational architecture, by which the data management is outsourced to an informational intermediary.
- Low-cost transponders, on which only an object ID is stored, can be utilised.

However, the following disadvantages can also be identified:

- Central systems distinguish themselves through poor scalability and the problem of a single point of failure: If there is a system failure at the central point of operations, then the entire supply chain is affected.
- In the case of central data management, questions of data ownership must be answered.

- A connection to the network is necessary.

Example: EPCglobal. A concrete example of the implementation of a decentralized data-on-network system is the EPC network [35]. The focus of the EPCglobal concept is the EPC (Electronic Product Code) number, with the help of which each transponder is allocated a unique identification number. The EPC constitutes the only information stored on the transponder. Other data pertaining to the object are deposited in external databases and referenced by means of unique identification numbers. The relay of the data to the relevant data source occurs by means of the Object Naming Service (ONS). The data sources are then offered by the EPC Information Systems (EPC IS). In order to facilitate the exchange of components between the EPCglobal network and external processes, the XML-based markup language PML (Physical Markup Language) was created [36]. The data retrieved from the readers is filtered and transformed by the middleware.

The data organization in distributed databases possesses the following advantages:

- The decentralized system is easily scalable.
- Compared with centralized data organization, data ownership is clearly regulated.
- Low-cost transponders can be utilized.

In addition to these advantages, however, the following disadvantages must be taken into account:

- Decentralized data organization represents a complex organizational architecture, above all requiring extended controls on identity and access.
- A connection to the network is necessary.

Data-on-Tag. The data-on-tag concept is based on the assumption that data that are needed for the creation of the abstract model in the information system are not necessarily gathered 'online'. On the contrary, they are captured at the point of action, which does not necessarily have to be within range of any network. Additionally, it is not always possible to make control data, which represent real world changes, available to the real world online. In such cases, the needed data must be physically present at the point of action [32]. Therefore, it lends itself to store the data on the tag, the data thereby accompanying the object. Thus, in the data-on-tag concept, the separation of physical objects from the data pertaining to them, as in conventional technologies and informational systems, is abolished.

Case study: Lemmi Fashion. The textile manufacturer Lemmi Fashion is equipping all of its clothing with RFID transponders, which, in addition to their unique IDs, contain data concerning size, color and other specific information, since the middle of 2005. The company is implementing RFID technology at the product level in its entire worldwide supply chain and, for this reason, belongs to the pioneers in the textile industry [3]. Passive transponders (with a frequency of 13.56 megahertz) are already being used at four different points in the clothes production and distribution process (the manufacturing facilities being located mostly in Asia): (1) as the products leave the manufacturing facility, (2) upon entering the distribution center, (3) in the transfer from quality control to the warehouse and (4) upon exiting the distribution center. In addition, several of Lemmi Fashion's customers have already announced their intention to implement an RFID infrastructure (5), whereby all supply chain participants would profit from the technology. This requires standardization of the memory's structure [37].

The data-on-tag concept is distinguished by the following advantages:

- No complex infrastructure or network connection is required.
- The organizational concept scales well by means of decentralized data management on the object itself (each object representing a small database).

The following disadvantages must be reckoned with:

- In the case that data on the tag is not stored redundantly, access to the data on a particular object is only possible when that object is physically present.
- The higher storage capacity of the transponders used in data-on-tag systems has the result that they are more expensive than those used in data-on-network systems.
- The data stored on the tag must be protected from unauthorized access.

The following figure summarizes and illustrates the advantages and disadvantages of the proposed concepts of data organization.

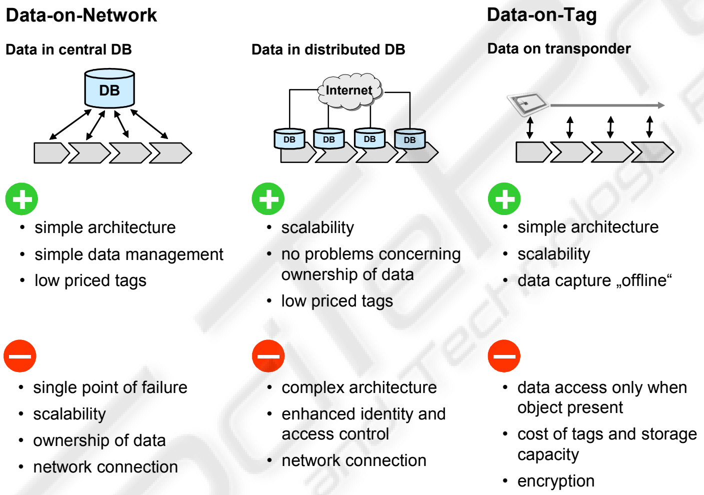

Fig. 1. Comparison of the concepts of data organization.

3.3 Data Security

The problem of data privacy and security plays a central role in the research on RFID, although the literature is primarily focused on the protection of personal consumer data (personal privacy) (e.g. [38] [39] [40]), corporate data security typically being neglected: "Industrial privacy, i.e., data secrecy, is important too, but less frequently considered" [41]. Indeed, the two areas of research are based on different considerations: While consumers are afraid of omnipresent surveillance (loss of privacy, objects being associated with people), companies are primarily interested in protecting company-internal data from unauthorized access and potential manipulation. However, the problems are not completely independent of one another, considering the fact that data security represents a required prerequisite in order to guarantee data privacy.

Especially in supply chains, the guarantee of data security is of primary importance, due to the fact that, in these complex systems, a great deal of (mostly insecure) cross company data exchange occurs. From the perspective of a participant in the supply chain, four primary threats to data security can be identified [42]:

Corporate espionage threat. Supply chain data can be spied out by competitors by querying transponders at designated places along the supply chain. Alternatively, communication can be bugged on the air interface. Both cases can lead to the evaluation of information from traffic patterns between transponders and readers (e.g. concerning the transmitted data quantity or the number of read sessions). Using information on goods movement, competitors can better formulate their own stocking strategies: 'Individually tagged objects could also make it easier for competitors to learn about stock turnover rates; corporate spies could walk through shops surreptitiously scanning items' [41]. A further threat is represented by so-called 'spoofing', in which transponders are imitated by the competitor in order to gain access to the transponder data, as well as so-called 'cloning' – the (unauthorised) capture of data and replication of transponders in order to, for instance, counterfeit high-value products [43].

Competitive marketing threat. By using objects outfitted with transponders, the unauthorized access by competitors of information on consumer preferences, which they can then use for their own personal marketing strategies, is made easier.

Infrastructure threat. The RFID infrastructure can, for example, be subjected to precise denial-of-service attacks, by which the sensitive flow of data can be disturbed. Physical attacks can, for example, consist of interrupting the flow of power to the reader(s) or excessive demands on the components. So-called 'shielding' represents another threat, in which the radio interface can be blocked by metal objects, or reduced by purposefully transmitting disruptive signals.

Trust perimeter threat. In supply-chain-wide RFID systems, large data volumes are being exchanged increasingly more often, which opens up more possibilities for competitors to intercept this information.

In order to guarantee the security of the data on tag, cryptographic protection measures, in particular, are being propagated [44]. This approach, however, has grave disadvantages:

- The implementation of cryptographic protection measures is associated with considerable costs. This represents a great challenge, particularly as it concerns identification at the product level, where the tag price plays an important role.
- Low-cost passive transponders do not have enough storage capacity for cryptography. And, although, according to Moore's Law, the storage and processing capacity of transponders will continue to grow, it is more likely that the

prices will fall in similar capacity classes than that new functionality will be offered at the same price [43].

- The implementation of cryptographic functions for the identification and authentication of data has the consequence that only transponders and readers which belong to a certain system are capable of communicating with one another. Because it is the goal of EPCglobal and ISO that the data stored on transponders be universally readable, traditional encryption methods are not suitable to protect the data from abuse.

In an effort to counter the problems just illustrated, a series of security measures are proposed in the literature. In order to secure low-cost transponders against counterfeit, a so-called 'relational check code' is proposed, with the help of which it can be ascertained whether data on the transponder were manipulated [45]. However, no determination can be made as to which part of the data was changed or to what degree the change occurred. The problem of counterfeit protection is also treated in [46]. The authors propose that the block of data comprising the unique object ID be used to deposit secret information (generated using three hash functions out of the data blocks Header, Object Class and Object ID) in this memory. Using this approach, it is possible to determine which data were manipulated. The proposed method has the advantage that no additional memory is required and, furthermore, no calculations are performed on the transponder.

Using the two security measures just illustrated, it is not possible to prevent counterfeit, only to discover it after the fact. In order to achieve an effective level of data security, active measures are necessary: Floerkemeier et al. describe the prototypical implementation of a 'watchdog tag', which monitors and records all reader activity in the proximity [47]. Rieback et al. propose the implementation of a device with the name 'RFID Guardian', which, similar to a computer firewall, intercepts reader queries and evaluates them before relaying them to the transponders [48].

In order to solve the problem of the 'competitive marketing threat', Juels proposes so-called 'pseudonym throttling' [43]. This is also a simple security mechanism which can be utilized in low-cost tags. The tag contains a short list of random IDs or pseudonyms. During each consecutive reading, the tag transmits the next available pseudonym from its list. In order to eliminate the danger that the list of pseudonyms is intercepted by multiple read queries performed within a short period of time, the tags are programmed so that they transmit their data with a predetermined delay.

3.4 Summary of Future Research Requirements

The following table summarizes the topics illustrated up to this point and gives an overview of suitable research questions relating to data management in the context of RFID-based supply chains.

Table 1. Overview of research questions.

Data collection and transformation
What consequences do demands on efficiency and accuracy have when choosing a type of data organization?
Extent of the data collection: What degree of visibility is economically reasonable?
How can the performance of the RFID data collection be adequately measured?
Into what form must the data be transformed for various information consumers along the supply chain?
To what extent should the data transformation process be decentralized? What problems result when extensive data transformation is already being conducted before relay to the applications?
Which traditional data warehouse concepts can be used in RFID systems? How can the data effectively be mined? What (potential) modifications must be made?
Data organization
What degree of decentralization is advantageous with respect to the proposed concepts?
Will new information intermediaries arise to manage the huge data volumes?
Which data should be stored on the object and which data should remain in databases?
Based on which rules should stored data be synchronized in a redundant data management system (data-on-network, as well as data-on-tag)?
Which supply chain steps are well-suited for 'object-accompanying' data storage?
How should the access concepts be regulated in a decentralized data management system?
Data security
What value do the data stored on the object represent for the company and what could competitors possibly do with the data?
How can data security be guaranteed while still maintaining the use of low-cost tags?
What alternative security measures could be employed instead of encryption (mainly because of costs and storage capacity)?
How can the RFID infrastructure be protected from denial-of-service attacks?
To what extent do additional security measures restrict the propagandized 'open' RFID systems?

4 Conclusion

Although RFID has entered supply chain management practice, the technology still poses several challenges that need to be addressed by research. In this contribution we discuss the particular challenges and possible solutions that practice faces in the field of RFID data management. The massive amount of potentially unreliable data is the main challenge in the field of data collection and transformation. Whereas progress has been made in the development of algorithms for the fast and reliable bulk reading, the improvement of these methods still constitutes a topic for future research in order to provide the accuracy and efficiency that practice requires. Other research opportunities remain in the field of data transformation, which deals with the question how raw and dirty data can be converted into information. Data organization persists to be of interest for research and practice. The recent inclusion of user memory in the standards of EPCglobal indicates a gain in importance of the data-on-tag concept. The extent of implementation of this decentralized approach as well as questions concerning the access of distributed data will be future objects of research. Data security faces severe challenges as research finds itself caught between the need for security measures and the necessity for simple and low priced tag architectures. This predicament intensifies when one considers possible effects of item-level tagging on consumer privacy. In response to early experiences from retailers who faced massive opposition when piloting item-level tagging, research needs to continue with the development of feasible security measures. In summary it can be ascertained that although RFID data management has been the object of intense research for the last few years, a variety of topics for future research remain.

References

1. Seidman, T.: The Race for RFID. The Journal of Commerce 4, 48 (2003) 16-18
2. Collins, J.: Metro Group reaps gains from RFID. RFID Journal (2005)
3. Speer, J. K.: Making (13.56) Waves. Apparel 2 (2006) 22-24
4. Michael, K., McCathie, L.: The Pros and Cons of RFID in Supply Chain Management. Proceedings of the International Conference on Mobile Business (2005) 623-629
5. Rao, J., Doraiswamy, S., Thakkar, H., Colby, L. S.: A deferred Cleansing Method for RFID Data Analytics. Proceedings of the 32nd VLDB Conference, Seoul (2006) 175-186
6. Jeffery, S. R., Alonso, G., Franklin, M. J., Hong, W., Widom, J.: Declarative Support for Sensor Data Cleaning. Pervasive Computing (2006) 83-100
7. Janz, B. D., Pitz, M. G., Otondo, R. F.: Information Systems and Health Care II: Back to the Future with RFID: Lessons Learned - Some Old, Some New. Communications of the Association for Information Systems 15, 7 (2005) 1-32
8. Cheong, T., Kim, Y.: RFID Data Management and RFID Information Value Chain Support with RFID Middleware Platform Implementation. Lecture notes in computer science, Vol. 3760, Springer-Verlag, Berlin Heidelberg New York (2005) 557-575
9. Zhang, X., Hu, T., Janz, B. D., Gillenson, M. L.: Radio Frequency Identification: The Initiator of a Domino Effect. Proceedings of the 2006 Southern Association for Information Systems Conference (2006) 191-196
10. Floerkemeier, C., Lampe, M.: RFID Middleware Design - Addressing Application Requirements and RFID Constraints. Proceedings of the 2005 joint conference on Smart objects and ambient intelligence, Grenoble (2005) 219-224
11. Wang, F., Liu, P.: Temporal Management of RFID Data. Proceedings of the 31st VLDB Conference, Trondheim (2005) 1128-1139
12. Babcock, B., Babu, S., Datar, M., Motwani, R., Widom, J.: Models and Issues in Data Stream Systems. Proceedings of 21st ACM Symposium on Principles of Database Systems (PODS 2002), June 3-5, 2002, Madison, Wisconsin (2002)
13. Hu, Y., Sundara, S., Chorma, T., Srinivasan, J.: Supporting RFID-based Item Tracking Applications in Oracle DBMS Using a Bitmap Datatype. Proceedings of the 31st VLDB Conference, Trondheim (2005) 1140-1151
14. Sarma, S.: Integrating RFID. QUEUE 10 (2004) 50-57
15. Hanebeck, C.: Managing Data from RFID & Sensor-based Networks. Retrieved from: www.globeranger.com/pdfs/futureoftheedge/GlobeRangerRFIDData.pdf (2004)

16. Shih, D., Sun, P.-L., Yen, D.C.: Taxonomy and Survey of RFID Anti-Collision Protocols. Computer and Communications 29, 11 (2006) 2150-2166
17. Spiekermann, S., Berthold, O.: Maintaining privacy in RFID enabled environments - Proposal for a disable-model. In: Robinson, P., Vogt, H., Wagealla, W. (eds.): Privacy, Security and Trust within the Context of Pervasive Computing. Springer-Verlag, Berlin Heidelberg New York (2005) 137-146
18. Hardgrave, B. C., Armstrong, D. J., Riemenschneider, C. K.: RFID Assimilation Hierarchy. 40th Annual Hawaii International Conference on System Sciences (2007)
19. Asif, Z., Mandiviwalla, M.: Integrating the Supply Chain with RFID: A Technical and Business Analysis. Communications of the AIS 15 (2005) 393-427
20. Vaidya, N., Das, S. R.: RFID-Based Networks – Exploiting Diversity and Redundancy. Technical Report (2006)
21. Finkenzeller, K.: RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. John Wiley & Sons, New York (2003)
22. Jain, S., Das, S. R.: Collision Avoidance in a Dense RFID Network. Proceedings of the 1st international workshop on Wireless network testbeds, experimental evaluation & characterization. ACM Press, New York (2006) 49-56
23. Kodialam, M., Nandagopal, T.: Fast and Reliable Estimation Schemes in RFID Systems. Proceedings of the 12th annual international conference on Mobile computing and networking. ACM Press, New York (2006) 322-333
24. Huang, X.: An Improved ALOHA Algorithm for Improved RFID Identification. Lecture Notes in Computer Science, Vol. 4253. Springer-Verlag, Berlin Heidelberg New York (2006) 1157-1162
25. Floerkemeier, C., Wille, M.: Comparison of Transmission Schemes for Framed ALOHA based RFID Protocols. International Symposium on Applications and the Internet Workshops (2006) 92-97
26. Myung, J., Lee, W.: Adaptive splitting protocols for RFID tag collision arbitration. Proceedings of the seventh ACM international symposium on Mobile ad hoc networking and computing. ACM Press, New York (2006) 202-213
27. Floerkemeier, C., Lampe, M.: Issues with RFID Usage in Ubiquitous Computing Applications. Lecture Notes in Computer Science, Vol. 3001. Springer-Verlag, Berlin Heidelberg New York (2004) 188-193
28. Jeffery, S. R., Alonso, G., Franklin, M. J., Hong, W., Widom, J.: A Pipelined Framework for Online Cleaning of Sensor Data Streams. Proceedings of the 22nd International Conference on Data Engineering (2006) 140
29. Jeffery, S. R., Garofalakis, M., Franklin, M. J.: Adaptive Cleaning for RFID Data Streams. Proceedings of the 32nd International Conference on Very Large Data Bases, Seoul (2006) 163-174
30. Gonzales, H., Han, J., Li, X., Klabjan, D.: Warehousing and Analyzing Massive RFID Data Sets. Proceedings of the International Conference on Data Engineering (2006)
31. Bornhövd, C., Lin, T., Haller, S., Schaper, J.: Integrating Automatic Data Acquisition with Business Processes Experiences with SAP's Auto-ID Infrastructure. Proceedings of the 30th VLDB Conference, Toronto (2004) 1182-1188
32. Diekmann, T., Melski, A., Schumann, M.: Data-on-Network vs. Data-on-Tag: Managing Data in Complex RFID Environments. 40th Annual Hawaii International Conference on System Sciences (2007)
33. Sarma, S.: A History of the EPC. In: Garfinkel, S., Rosenberg, B. (eds.): RFID – Applications, Security and Privacy. Addison-Wesley, Upper Saddle River, NJ (2006) 37-56
34. Trigg, J. B.: Progress for RFID: An Architectural Overview and Use Case Review. (2005)
35. Schuster, E. W., Allen, S. J., Brock, D. L.: Global RFID: the value of the EPCglobal network for supply chain management. Springer-Verlag, Berlin Heidelberg New York (2007)

36. Thiesse, F., Michahelles, F.: An overview of EPC technology. Sensor Review 26, 2 (2006) 101-105
37. Harmon, C. K.: The necessity for a uniform organisation of user memory in RFID. Int. J. RFID Technology and Applications 1, 1 (2006) 41-51
38. Garfinkel, S., Juels, A., Pappu, R.: RFID privacy: An overview of problems and proposed solutions. IEEE Security and Privacy 3, 3 (2005) 34-43
39. Henrici, D., Mueller, P.: Tackling security and privacy issues in radio frequency identification. In: Ferscha, A., Mattern, F. (eds.): Pervasive Computing. Lecture Notes in Computer Science, Vol. 3001, Springer-Verlag, Berlin Heidelberg New York (2004), 219-224
40. Spiekermann, S., Ziekow, H.: RFID: A 7-point plan to ensure privacy. European Conference on Information Systems (ECIS ’05), Regensburg, Germany (2005)
41. Juels, A.: RFID Security and Privacy: A research Survey. (2005)
42. Garfinkel, S., Juels, A., Pappu, R.: RFID Privacy: An Overview of Problems and Proposed Solutions. IEEE Security and Privacy 3, 3 (2005) 34-43
43. Juels, A.: Authentication and Identification - Minimalist Cryptography for Low-Cost RFID Tags. Lecture notes in computer science 3352, (2005) 149-164
44. Avoine, G.: Cryptography in Radio Frequency Identification and Fair Exchange Protocols. PhD thesis, EPFL, Lausanne (2005)
45. AVANTE International Technology: Supply Chain Security and Loss Prevention through Effective Counterfeit Prevention and Detection RFID Data Structure. (2005)
46. Potdar, V., Wu, C., Chang, E.: Intrusion Detection - Tamper Detection for Ubiquitous RFID-Enabled Supply Chain. (2005)
47. Floerkemeier, C., Schneider, R., Langheinrich, M.: Sensors and Tags - Scanning with a Purpose - Supporting the Fair Information Principles in RFID Protocols. Lecture notes in computer science, Vol. 3598, Springer-Verlag, Berlin Heidelberg New York (2005) 214-231
48. Rieback, M. R., Crispo, B., Tanenbaum, A. S.: Mobile Security - RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management. Lecture notes in computer science, Vol. 3574, Springer-Verlag, Berlin Heidelberg New York (2005) 184-194