MIT Libraries | DSpace@MIT

MIT Open Access Articles

Technology, standards, and real-world deployments of the EPC network

The MIT Faculty has made this article openly available. ***Please share*** how this access benefits you. Your story matters.

Citation: Thiesse, F. et al. “Technology, Standards, and Real-World Deployments of the EPC Network.” Internet Computing, IEEE 13.2 (2009): 36-43. © Copyright 2009 IEEE

As Published: http://dx.doi.org/10.1109/MIC.2009.46

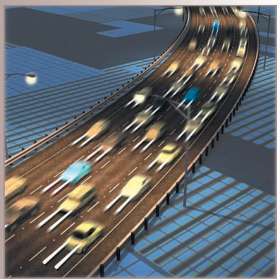
Publisher: Institute of Electrical and Electronics Engineers

Persistent URL: http://hdl.handle.net/1721.1/62248

Version: Final published version: final published article, as it appeared in a journal, conference proceedings, or other formally published context

Terms of Use: Article is made available in accordance with the publisher's policy and may be subject to US copyright law. Please refer to the publisher's site for terms of use.

Massachusetts Institute of Technology



Editors: Frédéric Thiesse • frederic.thiesse@unisg.ch
Florian Michahelles • fmichahelles@ethz.ch

Technology, Standards, and Real-World Deployments of the EPC Network

The EPC Network is a global RFID data sharing infrastructure based on standards that are built around the Electronic Product Code (EPC), an unambiguous numbering scheme for the designation of physical goods. The authors present the fundamental concepts and applications of the EPC Network, its integration with enterprise systems, and its functionality for data exchange between organizations in the supply chain.

Frédéric Thiesse
University of St. Gallen

Christian Floerkemeier
Massachusetts Institute of Technology

Mark Harrison
University of Cambridge

Florian Michahelles
ETH Zurich

Christof Roduner
ETH Zurich

In recent years, the Electronic Product Code (EPC) — a worldwide, unambiguous code for the designation of physical goods — has become the subject of enormous interest, not only in research but also in several industries and society in general. The rapid and escalating diffusion of the EPC was particularly driven by the Auto-ID Center, a project to develop RFID standards founded in 1999 at the Massachusetts Institute of Technology (MIT) with cooperation from numerous industrial sponsors.[1] The Auto-ID Center created the EPC to ensure RFID interoperability in supply-chain-wide applications. An important feature is its capability to serve as a meta-scheme that integrates with existing numbering schemes, such as the serialized Global Trade Item Number (GTIN) standard used in retail. However, the Center's long-term objective wasn't only standardizing numbering formats but also developing an entire family of open standards, including air interface protocols, software interfaces, and directory services, to bridge the gap between the physical and virtual worlds.[2] In October 2003, the Auto-ID Center was transformed into an international research network known as Auto-ID Labs, which concentrates on technology as well as application-oriented research, and EPCglobal, a nonprofit organization responsible for commercializing, standardizing, and managing EPC standards.

 1089-7801/09/$25.00 © 2009 IEEE

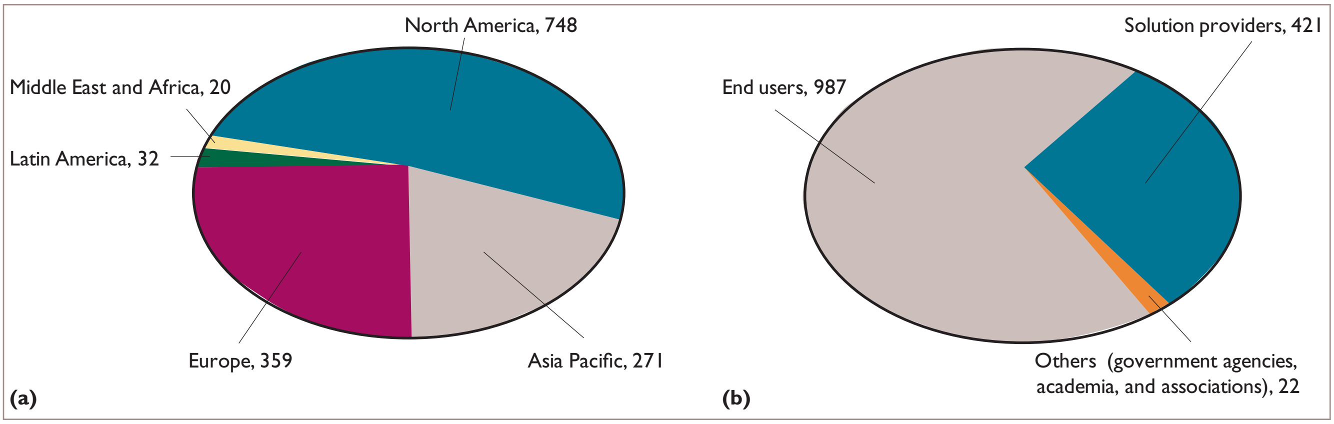


Figure 1. Member companies of EPCglobal by (a) region and (b) industry sector (as of November 2008).

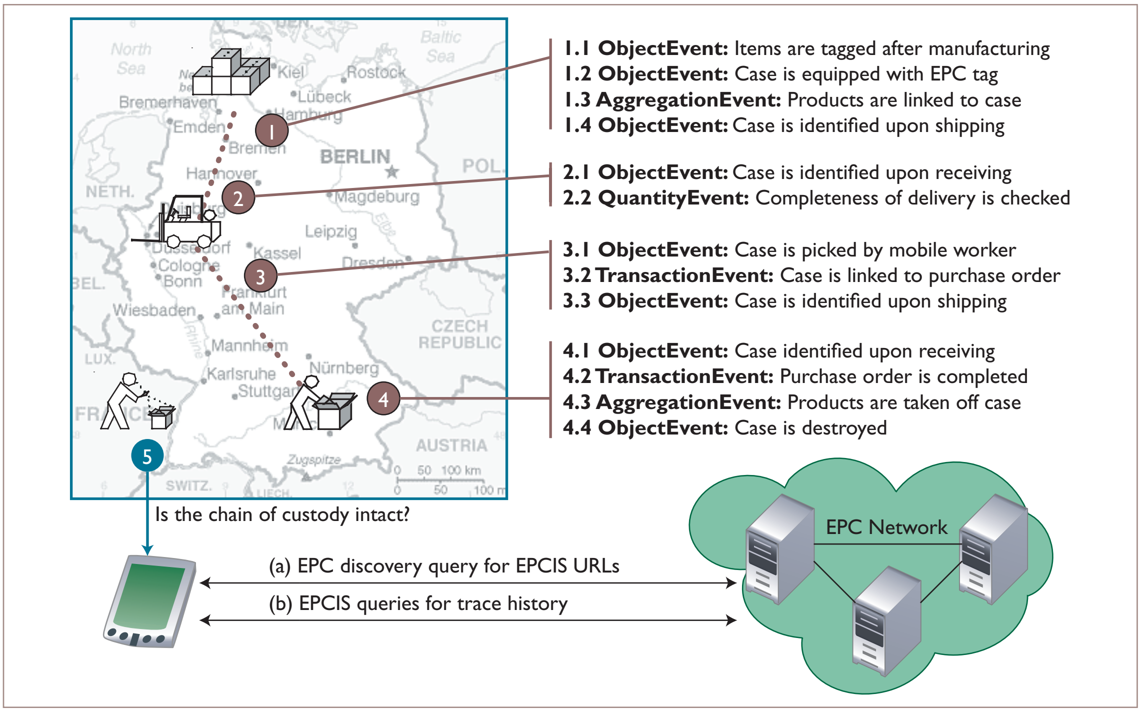


Figure 2. The physical flow of goods is tracked along the supply chain, which lets consumers reconstruct a product's history and verify its origin.

In the years that followed, EPC technology became the technical foundation for several large chain stores' RFID initiatives — Wal-Mart and Metro, for instance — as well as for industrial enterprises and government organizations such as Pfizer or the US Department of Defense, respectively. As Figure 1 shows, the number of EPCglobal subscribers has reached 1,430, with several in the US, where most large consumer goods manufacturers are based, followed by Germany and Japan. Within the EPCglobal community, several working groups discuss technical requirements, develop business cases, and establish standards to promote the introduction of the EPC worldwide. The common framework for these activities is the EPC Network Architecture,[3] which includes specifications that deal with the collection of captured data and their distribution across organizations (see Figure 2). From the outset, the EPC Network's underlying philosophy has been to build a federated system — that is, to provide an RFID application infrastructure rather than the application itself. However, the initial standards development focused more on the EPC Network's lower levels than on data exchange across supply chains.

Tags and Readers

One of the Auto-ID Center's primary objectives was to develop air interface protocols and tag manufacturing technology that allowed for low-cost tags. The availability of low-cost RFID technology would allow RFID use beyond traditional niche applications. Although tags are still slightly more expensive than initially envisioned, it was the establishment of global standards for low-cost tags — most of all, the ratification of the EPC Class 1 Generation 2 (Gen2) standard in 2004[4] — that led to a massive price decline for transponder inlays from more than US$1 in the 1990s to less than $0.10 in 2006. In contrast to its predecessor, Gen2 came with higher read rates, an improved anti-collision protocol, support for user memory, and other features that fueled rapid adoption. Furthermore, the standard also included a so-called "kill command" for permanent tag deactivation to address the fears of an increasingly privacy-aware public. In 2006, the International Organization for Standardization (ISO) approved Gen2 as ISO/IEC 18000-6C, an important prerequisite for future acceptance of the standard in industries other than retail, such as the automotive and aerospace industries.

In the EPC Network Architecture, the *reader protocol* (RP), a reader API that abstracts entirely from the underlying hardware, determines access to RFID reader devices. RP is complemented by the *reader management* (RM) protocol, which allows for the naming of readers and locations, the generation of statistics on RF operations, and so on. However, it soon became evident that, against the background of Gen2's growing success in the market, users hardly perceived the advantages of hardware abstraction as crucial factors. Even worse, the lack of control over the air interface made the standard seem inappropriate for use in harsh environments where acceptable read rates require finely tuned configuration of hardware parameters. Consequently, EPCglobal released an alternative low-level reader protocol (LLRP) specifically designed for full Gen2 support shortly afterward.

The sheer mass of raw data generated by even a few readers can easily result in an unacceptable load for corporate networks and systems. For this reason, an additional middleware layer is needed that filters the data collected from readers already on the network's edge. In the EPC Architecture, this task is supported by the *application-level events* (ALE) interface, which hides the RFID infrastructure's details — or any other identification technology's details — from client applications. First, ALE allows for consolidation of observations over time; that is, the conversion of a series of tag reads into a single event message with a time interval attribute. Second, the standard supports the declaration of logical readers that bundle the data streams from multiple physical readers, such as occurs in larger areas that can't be covered by a single reader alone.

EPC Information Services

In traditional RFID applications, such as access control and animal identification, tags moved in closed-loop processes, and the RFID data was consumed only by a single client system. Accordingly, there was little need for disseminating data across organizational boundaries. However, in the same way as monolithic business information systems of the past have evolved into highly networked systems that use the Internet extensively, RFID is increasingly deployed in supply-chain-wide applications with readers that are distributed across factories, warehouses, and stores. This is where EPC Information Services (EPCIS) comes into play as a common interface standard for data transfer between systems.

EPCIS information helps business applications understand how and why physical events occurred and what state objects are in.[5] At its core, EPCIS might provide a repository of historical tag events and related information that is fed by an EPCIS *capturing application*, such as an inventory management system that is connected to ALE-compliant middleware. On the other hand, EPCIS can be queried by an EPCIS *accessing application*, such as another internal system or an authorized external party. The query interface allows for sending one-off queries as well as for subscribing to long-running standing queries that are answered periodically by asynchronous callbacks.

The way in which an EPCIS sees the world is determined by four different event types in its abstract data model, which Table 1 shows. An `ObjectEvent` corresponds to the detection of one or more EPC-equipped items, such as on a dock door on arrival of a shipment. Because the granularity of individual EPC identification isn't always needed, a `QuantityEvent` can

Table 1. EPC Information Services Event types and attributes.							
		EPCISEvent (base class)	**Object-Event**	**Aggregtion-Event**	**Quantity-Event**	**Transaction-Event**	
When?	eventTime	●	●	●	●	●	Time of event observation
	recordTime	❍	❍	❍	❍	❍	Time of event registration
	eventTimezone-Offset	●	●	●	●	●	Time zone information
What?	epcList		●			●	List of observed EPCs
	parentID			❍		❍	Containing object ID
	childEPCs			●			Contained objects IDs
	epcClass				●		Product type
	quantity				●		Number of observed objects
	action		●	●		●	Life-cycle phase of the EPCs
Where?	readPoint		❍	❍	❍	❍	Reader name
	bizLocation		❍	❍	❍	❍	Location name
Why?	bizStep		❍	❍	❍	❍	Business process step
	disposition		❍	❍	❍	❍	State of the objects
	bizTransactionList		❍	❍	❍	●	Associated transactions

● = mandatory, ❍ = optional

alternatively be used that includes only information on the product type and the number of objects, which equals the level of detail obtained from barcode scanning. In contrast, an `AggregationEvent` isn't associated with a particular tag read but rather denotes a (dis-)aggregation of a group of items, such as cases that are put on a pallet for shipping. In a similar way, a `TransactionEvent` links EPCs to a specific business transaction, such as a purchase order. To enrich events with their business context, the EPCIS repository also includes master data such as the names of business locations, process steps, and transactions. Some of these vocabularies aren't predefined by the standard itself but are rather the result of industry- or company-specific agreements.

To find EPC-related information, business applications use the Object Name Service (ONS) to provide an EPCIS URL when queried with a tag's EPC. The ONS shares the same hierarchical design as the Internet Domain Name System, with queries being delegated from a global root server down to local instances of individual organizations. Because the ONS is allowed only to point to the manufacturer's EPCIS repository, the EPC Network is being extended to include EPC Discovery Services. These services will allow applications to find third parties' EPCIS repositories across an object's individual supply chain, which can then provide detailed event information to others. It's likely that multiple discovery services will coexist in the future, equipped with additional mechanisms for cooperation and awareness of each other.

In many settings, EPC Network applications will also be integrated with existing infrastructures for electronic data interchange (EDI). This is achieved by extending EDI message standards with additional data fields on EPC codes. GS1, the organization responsible for EANCOM (International Article Numbers, formerly European Article Numbers) standards, a subset of the electronic data interchange standards (UN/EDIFACT) used in retail, was the first to propose synchronizing EDI with EPC data.[6] The proposal defines a dispatch advice message that includes the EPC codes of logistical or sales units as well as other information on shipped orders. Figure 3 depicts the sequence of information flow in the shipping and receiving process of a delivery using RFID tagging on logistical units, which are equipped with EPC tags that store serial shipment container codes (SSCCs). In this case, RFID is used for automatic completeness checks of outgoing shipments at the supplier's site and incoming shipments at the retailer, whereas EDI is used as a medium to actively transmit EPC

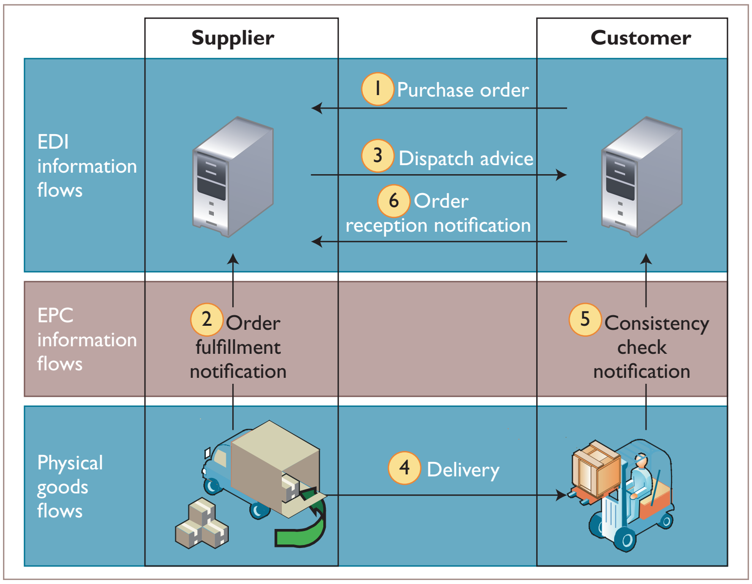


Figure 3. Electronic data interchange communication between suppliers and retailers is complemented by RFID/EPC data.

and other order-related data from one company to another.

Real-World Applications

The rationale for existing RFID implementations usually follows the logic of process acceleration — that is, the value of RFID is mostly in time and labor savings. Prohibitive technology costs, however, inevitably limit the number of economically feasible applications. In contrast, the EPC Network shifts the focus to the value of data to a company's operations. In retail, for instance, ordering decisions based on point-of-sale (POS) and coarse-grained inventory data might be improved through real-time information on goods in transit and shelf inventories. The underlying idea is shown in proprietary centralized systems such as Wal-Mart's Retail Link. In the EPC Network, however, events remain distributed and are shared only on an on-demand basis; thus, each trading partner keeps its data. A number of research initiatives and pilot projects are currently under way to investigate the resulting benefits in detail.[7]

An example is the trial at the German-based Galeria Kaufhof department store chain, which demonstrates how RFID can be used to optimize processes in retail stores. In its store in Essen, Germany, roughly 30,000 individual articles of clothing and accessories in the 2,000-square-meter men's apparel department are equipped with hangtags embedded with EPC Gen2 labels. The entire floor is equipped with roughly 60 stationary EPC-compatible readers at the exits, escalators, fitting rooms, cash desks, and selected shelves. Employees are equipped with mobile readers for inventory counts and customer service. The software infrastructure includes an EPC Network installation with a business intelligence tool that can access EPCIS, which provides inventory information and other key indicators. The trial's objective is not only to improve existing in-store processes but also to give store managers insight into customer behavior beyond traditional POS data. One key indicator that stores can derive from EPC events is the ratio of try-ons and sales, for instance, which allows the store to draw conclusions about its assortment of merchandise down to individual items.

Another promising candidate for future EPCIS killer applications is coming from a completely different direction. The phenomenon of counterfeits has become a threat to brand manufacturers that not only affects drugs and designer clothes but has also spread to many other product categories. Moreover, classic security features, such as holograms, can increasingly be copied as well. The impact of fake products includes lost sales, erosion of brand value, liability claims, and so on. Against this background, producers of pharmaceuticals, car parts, luxury goods, and high-value consumer goods are among the main adopters of RFID-based tracking and tracing with EPC technology.

Figure 4 shows an EPC-equipped case filled with a number of sales units carrying EPC tags. At the manufacturer's dock, the case is identified for the first time and shipped out. The wholesaler receives the case, scans its EPC, verifies the number of units, and stores it in his or her distribution center. When the wholesaler gets an order from a retailer, the case is picked up by a worker in the distribution center, linked to the order number, and identified a second time on shipping. The retailer scans the EPC of the case and its contents when its received and completes the order transaction. The sales units are brought to the store's backroom, and the case is destroyed. If one of the products later appears at a different place, customs officials or consumers can verify whether the EPC has been issued, if the item has taken a suspicious route, whether the product history is complete, and so on. The benefit from RFID is twofold:[8] the ID tag itself becomes a product-identity fea-

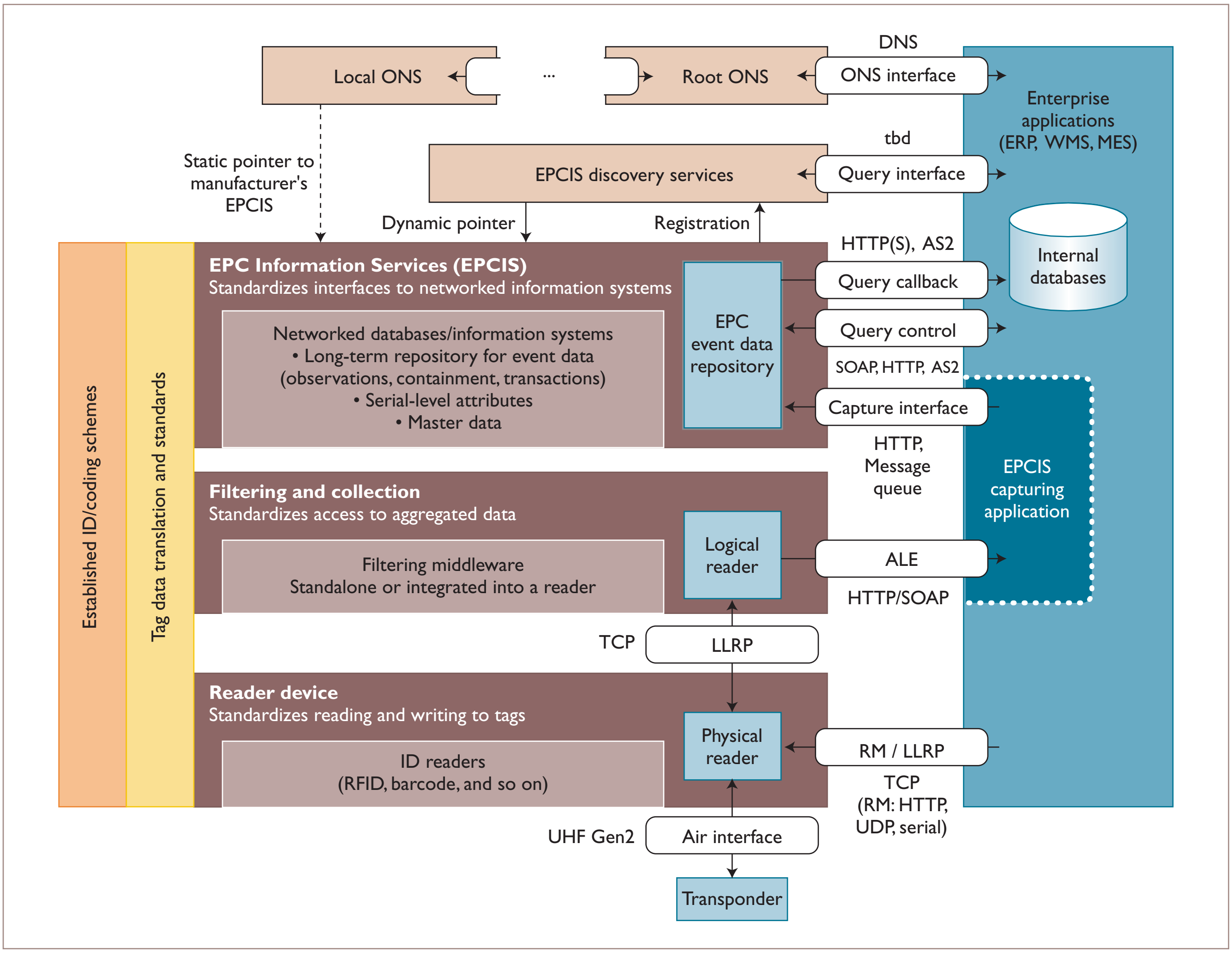


Figure 4. Overview of the main components and interfaces of the EPC Network Architecture.

ture that indicates whether a product is genuine, and the trace data stored in different EPCIS instances allows users to reconstruct its history. Thus, manufacturers and retailers could detect counterfeits that are equipped with stolen or copied tags because their EPCIS traces won't match their physical location.

Outlook

Despite the considerable growth of the EPCglobal subscriber base in recent years, the EPC technology adoption process is still in its infancy compared to traditional bar code technology. One important driver that might foster future diffusion of EPC standards is open source implementations of the EPC Network stack. Recently released EPC Network specifications such as LLRP, Tag Data Translation, and EPCIS provide standardized interfaces to core services in an RFID deployment. The competitive advantage to a business from implementing these specifications is thus diminishing and is increasingly viewed as a point of collaboration. The LLRP toolkit project (www.llrp.org) is a good example of this trend in which reader vendors no longer see a competitive advantage in developing individual client libraries for the same standardized protocol, looking for collaboration to lower cost instead. The lower development cost will, in turn, lower the cost of the overall solution for the customer — increasing the market for the technology and promoting the use of the standardized interface. The availability of open source EPC Network standards implementations — Fosstrak (www.fosstrak.org), for example — is also beneficial in education and research. In education, universities get access to free implementations of the standards, facilitating use in seminars and labs.[9] In research, the availability of free EPC Network software lets researchers in academia and enterprises experiment with the standards and suggest novel implementations and future extensions.[10]

To realize the original vision of a global RFID data exchange infrastructure, however, academia and industry must overcome several future challenges. The first refers to technology and standards. It remains to be seen if the architecture is scalable enough to handle thousands of EPCIS servers managing trillions of EPC-equipped items that generate not only RFID events but also sensor and location information. This issue might conflict with some users' demands for a powerful but resource-intensive EPCIS query language. On the other hand, the standardization process will become more complex with an increasing number of application requirements. The EPCglobal community has made significant progress in the development of RFID and networked information systems, with more than 10 ratified standards. However, as different working groups develop different standards, there is the danger of producing competing or overlapping standards. Time will tell whether EPCglobal succeeds in further developing new features of the EPC Network while keeping the framework a consistent whole.

Many RFID applications require substantial changes in existing information systems to turn raw tag data into meaningful information. A premise for RFID-based inventory management in retail stores, for instance, is linking the EPC with existing POS and merchandise-management systems. The quality of product-related master data in these systems, however, usually doesn't meet the detail level that users require from RFID to make better decisions on inventory levels and shelf replenishments.[11] As in the case of the Galeria Kaufhof trial, one of the challenges in practice is that information on many items is only available at the product category level, such as a specific manufacturer's shirts. More fine-grained information on size and color that could be linked to the EPC is often not available from suppliers or from the company's own purchase department. Similar problems arise in grocery retail and other industries in which master data management is still a major issue despite the increasing use of common data pools.

The economic value of data sharing is still not fully understood. In recent years, numerous white papers, trade publications, and research reports have discussed RFID benefits. A widespread belief has been that RFID would somehow revolutionize current practices in supply-chain management. Unfortunately, most of these estimates have yet to be substantiated,[12] and some businesses that try to justify RFID might not even need it.[13] Although it's relatively straightforward to estimate the costs of an RFID infrastructure, it's usually difficult to quantify the benefits beyond simple handling-efficiency gains. In counterfeit cases, for example, substitution effects and the long-term impact on brand value are largely unknown, even to affected companies. Moreover, provided that the benefits are evident, questions remain about data ownership and cost sharing among supply-chain partners. As observed at many of today's EDI deployments, both issues are highly political and depend more on trust and other soft factors than on the technology itself.

EPC Network users might sooner or later be facing a variety of security issues.[14] Owing to its heritage, the ONS shares the benefits of the DNS, but is also prone to denial-of-service attacks and cache poisoning.[15] Furthermore, the network isn't only threatened by hackers but also by fraudulent insiders. EPCIS events reflect a company's supply chain structure and, once disclosed, let competitors draw conclusions on inventory levels, lead times, cost structures, and other sensitive data. In this scenario, valuable information could easily be collected by guessing a large number of EPCs and querying the corresponding EPCIS servers. Even if EPCIS access is limited, knowing the list of servers that hold information on an item from a discovery service query already poses a possible security problem. A solution might include not publishing these results explicitly but encapsulating EPCIS servers such that all EPCIS queries are routed through the discovery service, or developing portable fine-grained access control policies that can be enforced at both the EPCIS and discovery service query interfaces.

With the growing number of RFID implementations, it's foreseeable that privacy activists, who have been warning against omnipresent surveillance via RFID for years, will intensify their efforts. Indeed, EPC technology addresses privacy through the password-protected Gen2 kill command. However, the management of password data along the supply chain, which is necessary to prevent unauthorized mass tag deactivation, is still an unresolved issue.

All these issues pose major challenges that the RFID/EPC community will have to cope with to ensure the global EPC Network's long-term success. On a larger scale, however, these issues might only be the first steps toward an even bigger vision. Low-cost sensors, real-time location systems, and other pervasive technologies are already underway to complement RFID, thus creating a world of smart and interconnected physical objects: the Internet of Things.

References

1. S. Sarma, "A History of the EPC," *RFID: Applications, Security, and Privacy*, S. Garfinkel and B. Rosenberg, eds., Addison-Wesley, 2005, pp. 37–55.
2. D. Brock, "The Electronic Product Code (EPC) – A Naming Scheme for Physical Objects," white paper, Auto-ID Labs (AUTO ID-WH-002), 2001.
3. K. Traub et al., "The EPCglobal Architecture Framework," EPCglobal, 2005; www.epcglobalinc.org/standards/architecture/.
4. "EPC Radio-Frequency Identity Protocols, Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.0.9," EPCglobal, 2005; www.epcglobalinc.org/standards/uhfc1g2.
5. "EPC Information Services (EPCIS) v. 1.0," specification by EPCglobal, 2007; www.epcglobalinc.org/standards/epcis.
6. "GS1 EDI Recommendation for Transmission of EPC's SSCC & SGTIN Coding Schemes," GS1 Global Office, 2008; www.gs1.org/docs/gsmp/eancom/EDI_Recomendation_EPC_SSCC_SGTIN.pdf.
7. B. Violino, "Leveraging the Internet of Things," *RFID J.*, Nov./Dec. 2005, pp. 18–27.
8. T. Staake, F. Thiesse, and E. Fleisch, "Extending the EPC Network – The Potential of RFID in Anti-Counterfeiting," *Proc. 20th Ann. ACM Symp. Applied Computing*, ACM Press, 2005, pp. 1607–1612.
9. C. Floerkemeier, C. Roduner, and M. Lampe, "RFID Application Development with the Accada Middleware Platform," *IEEE Systems J.*, vol. 1, no. 2, 2007, pp. 82–94.
10. E. Grummt and M. Mueller, "Fine-Grained Access Control for EPC Information Services," *Proc. 1st Int'l Conf. the Internet of Things*, Springer, 2008, pp. 35–49.
11. C. Legner and J. Schemm, "Toward the Inter-organizational Product Information Supply Chain – Evidence from the Retail and Consumer Goods Industries," *J. Assoc. Information Systems*, 2008, pp. 120–152.
12. H. Lee and Ö. Özer, "Unlocking the Value of RFID," *Production and Operations Management*, vol. 16, no. 1, 2007, pp. 40–64.
13. J. Woods, "Use RFID Only If It's Intrinsic to the Business Case," Gartner Research, 2003.
14. D. Konidala, W.-S. Kim, and K. Kim, "Security Assessment of EPCglobal Architecture Framework," white paper, Auto-ID Labs (WP-SWNET-017), 2006.
15. B. Fabian, O. Günther, and S. Spiekermann, "Security Analysis of the Object Name Service for RFID," *1st Int'l Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing*, 2005; www.taucis.hu-berlin.de/_download/security_analysis.pdf.

Frédéric Thiesse is a project manager at the Institute of Technology Management and associate director of the Auto-ID Lab at the University of St. Gallen. His research interests include RFID applications. Thiesse has a PhD in business administration from the University of St. Gallen. He is a member of the Association for Information Systems. Contact him at frederic.thiesse@unisg.ch.

Christian Floerkemeier is associate director of the Auto-ID Labs at the Massachusetts Institute of Technology. His research interests include RFID and pervasive computing. Floerkemeier has a PhD in computer science from ETH Zurich. He is a member of the IEEE and program chair of IEEE RFID 2009. Contact him at floerkem@mit.edu.

Mark Harrison is director of the Auto-ID Lab at the University of Cambridge. His research interests include architectures for networked RFID, discovery services, and enhanced track and trace techniques. He has a PhD in physics from the University of Cambridge. Contact him at mark.harrison@cantab.net.

Florian Michahelles is a project manager at the Department of Management, Technology, and Economics and associate director of the Auto-ID Lab at ETH Zurich. His research interests include RFID, human-computer interaction, and Internet of Things applications for consumers. Michahelles has a PhD in computer science from ETH Zurich. He is a member of the IEEE. Contact him at fmichahelles@ethz.ch.

Christof Roduner is a doctoral researcher at the Institute for Pervasive Computing and the Auto-ID Lab at ETH Zurich. His research interests include middleware for RFID systems, infrastructures for smart objects, and human-computer interaction. He is one of the cofounders of the Fosstrak project, an open source RFID middleware. He holds an M.Sc. degree in computer science from the University of Zurich. Contact him at roduner@inf.ethz.ch.