The EPC Business Collaboration Framework

Thoughts on the Future Role of the EPC Network

Alexander Ilic, Florian Michahelles, Elgar Fleisch

Auto-ID Labs White Paper WP-SWNET-021

Alexander Ilic
Senior Researcher
ETH Zurich

Florian Michahelles
Associate Director
Auto-ID Labs ETH Zurich

Elgar Fleisch
Research Director
Co-Chair of Auto-ID Labs
University of St.Gallen and ETH Zurich

Contact:

Auto-ID Labs ETH Zurich/St.Gallen
Swiss Federal Institute of Technology (ETH) Zurich
Department of Management, Technology, and Economics
Kreuzplatz 5
8032 Zurich
Switzerland

Phone: +41 44 632 89 83
Fax: +41 44 632 10 45

E-Mail: ailic@ethz.ch
Internet: www.autoidlabs.org

Software & Network

Index

Abstract

This paper presents some early thoughts on the future role of the EPC Network. We embrace the idea of linking information sharing aspects of Supply Chain Management with the EPC Network. By analyzing the functionality of the EPC network against common mechanisms of business coordination, we identify the need for additional software layers, necessary to transform the EPC network into a business collaboration framework.

1. Introduction

The reason why companies deploy RFID solutions is clearly to improve the efficiency of business processes [8]. With globally unique numbering schemes, such as the Electronic Product Code (EPC) [11], organizations can store and share information about item movements with regards to their business context. Examples range from intra-organizational to inter-organizational applications and include the optimization of logistics operations, automatic inventory adjustments [6], or even the ability to detect counterfeits [10].

Today, the Internet represents a basic communication channel that connects organizations from all over the world. The idea of networked RFID is to use this existing infrastructure to exchange RFID-based trace data and thus enable efficient business collaborations on a global scale. A first step towards that direction is the so-called EPC network architecture [11], which tries to standardize components and interfaces relevant for RFID-supported business processes. Currently, only the lower level components (i.e. tag, reader, middleware) specified in the EPC network architecture are being used in actual implementations [12]. This implies that, currently, the EPC network architecture does not play a relevant role in inter-organizational exchange of RFID trace data. However, there are already some small and closed-loop applications, in which organizations collaboratively exchange RFID trace data [9]. In order to exchange data on the network, these organizations are, however, forced to use proprietary software to connect their local EPC network stacks and their businesses thereof. The lack of standardization and high costs for developing common components over and over again is hereby a major hindering factor for the adoption of RFID [8].

For the remainder of this document, we define RFID trace data as the event data that is generated by interrogating a RFID tag (attached to a logistic object), which is enriched by context information (such as the business context, location information) at the reader or middleware level. In contrast to classical information sharing systems such as EDI systems, which only coordinate and automate the exchange transactional information [4] (e.g. orders, prices, product specifications, quality specifications, or delivery specifications), the exchange of RFID trace data comprises high resolution item information and therefore actual “footprints” of business processes. The value of this information is in most cases not yet leveraged [6].

The goal for this article is therefore to analyze the EPC network and identify additional layers necessary to transform the EPC network into a large-scale business collaboration framework.

2. Business Collaboration Framework

In this Section, we introduce the idea of our EPC business collaboration framework. The framework analyzes and enhances the EPC Network in two categories: 1) enabling information sharing and 2) supporting business through RFID trace data. The first category aims to support routine tasks for establishing information sharing relationships. While the first category is more technically driven, the focus of the second category is to look at the EPC network from a business point-of-view. In following the Service-oriented Architecture (SoA) paradigm [2], we structure the second category as operational, tactical and strategic layers. The goal is to illustrate that future RFID applications can be valuable far beyond the sole support of operational tasks (e.g. track and trace) by having a standard components also for high-level needs. For this short paper, we do not discuss how our architectural proposal may be fulfilled. There may already exist commercial or non-commercial applications that complement or fulfil parts of our architecture. Therefore, we want to focus on the big picture and discuss the architecture from a point-of-view, where all parts of the architecture could be commodities that seamlessly play together through standardized interfaces.

To support our idea, we propose a high-level and layered architecture for the EPC business collaboration framework as depicted on Figure 1. In the following, we will guide the reader through this proposal from the bottom to the top layers.

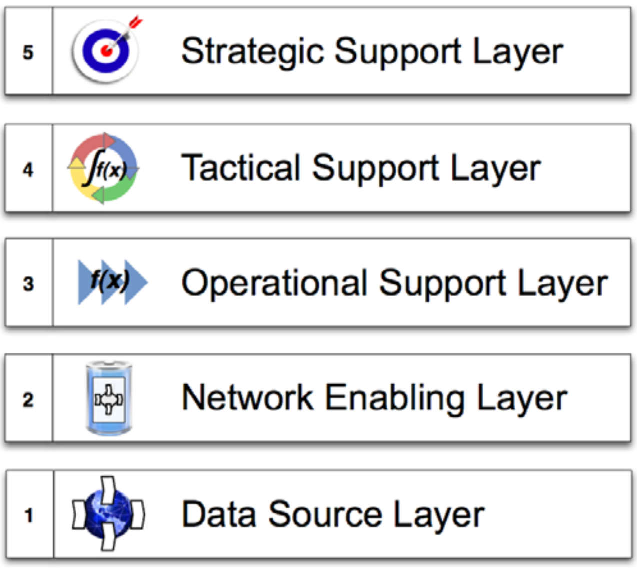

Figure 1. Proposed layers for a EPC-based business collaboration framework on top of the local EPC Network stack

2.1. Data source and network enabling layers

The "data source" layer in Figure 1 represents the top layer of the existing EPC architectural specification. It contains data sources accessible through the recently ratified interfaces from and to EPCIS data repositories [1]. These data sources contain the RFID data traces intended for inter-organizational information sharing. In contrast, "network enabling" layer has the role of supporting the information exchange. As the name suggests, services in this layer should enable the seamless and interoperable operation of EPC-based information sharing networks. Services may ensure the linkage of distributed data sources, translate between different types of information, or provide other meta-services. In the following, we will detail the role of this layer by analyzing the EPC network against the common concept of business coordination (as described in [5], [3]). Hereby, we want to explain how successful inter-organizational data transactions can be achieved with services and standards. While local standards may be sufficient for proprietary closed-loop applications, the following steps for coordinating services in the "network enabling" and "network access" layers reveal the needed amendments to achieve a smooth integration.

Step 1: Find partner

In a data-driven architecture, the most challenging goal is to find trace data providers. Currently, the Object Naming Service (ONS) provides basic lookup capabilities to find the EPCIS data source encoded in the tag's manager number. However, the ONS cannot return information about other data sources (e.g. other partners in a supply-chain than the manufacturer and creator of the EPC), which may hold information about an object as well. Therefore the concept of EPC Discovery Services (EPCDS) was introduced to find any data source that contains information about a specific object identified by its EPC. Today, the specification of the EPCDS is still on going.

Step 2: Authenticate partner

Business collaboration requires established means of authenticating partners in order to verify the claimed identity of the partners. However, unlike web search engines, the services like EPCDS should not return response data directly. They need to rely on mutual authentication to ensure that the service transaction is conducted in a secure environment. Despite concepts like a Public-Key Infrastructure (PKI) based on X.509 certificates are mentioned in the EPC network specification [11], there is no proposal how to efficiently manage the certificates and their association to the partners. It must be ensured that the digital identities map to identities in the real world and the assignment of certificates bases on a fair process. We propose therefore an additional component that helps to manage and verify signatures of authorized members of the EPC network.

Step 3: Coordinate method

Before conducting the service transaction, it must be clear what access goals the service user has. For example, is the intention to change data or to read data? For this reason, access control mechanisms should be implemented. While almost all companies want to make sure that they are in full control about the data that they have stored in their repositories, interoperability is a key issue. Services or standards must create ways to bridge from one access control policy of a particular company to another. Additionally, the access management system must be very efficient and scalable to handle permissions for item-level data.

Step 4: Coordinate service

For the service transaction itself, it must be clear, whether this is a one-time occurrence or a repeated access. Also the agreement about service termination must be clear. Companies will not share information, if the objectives are not clearly defined. Services should therefore restrict general access to data for specific purposes only.

2.2. Business supporting layers

While the previous category discussed technical service coordination and integration steps, the following part walks through the business layers (cf. Figure 1) that link the aforementioned technical infrastructure with the support of operational, tactical or strategic processes.

Operational Layer

Services in this layer aim to support the efficiency on the operational level. On a supply chain perspective, this translates into strengthening the execution of a particular link. As usually only two parties, namely buyer and seller, are involved, the data exchange will be mainly take place between these two parties. Operational data [7] that is exchanged in this context can help to determine inventory levels, shipment allocations, trace histories (such as the E-Pedigree), or item specific location information. If a service is designed to use the underlying data to support business operations, it is required that the service is accessible during the whole business hours. Availability is a very critical property. These RFID-based services are likely to be embedded directly into process work flows. If the employees get no response from these services, a live process could be blocked. An example would be a routine product verification check for all received goods based on an anti-counterfeiting service.

Tactical Layer

Services in the tactical layer have the goal of supporting managerial decision making on a tactical level by working on a more aggregated data level. To gain tactical data, probably more data sources than in the operational layer need to be accessed. If more and more processes base on RFID trace data, it can be expected that for an optimal management of these processes this dedicated layer is valuable to determine the operational effectiveness. Data that is generated by the business operations layers can directly be evaluated and compared in a "as is" versus "to be" fashion. Services in this layer keep track of the performance and monitor operations on a broader scope. Therefore, increased transparency and clear output characteristics are needed. This will enable managers to support their decisions regarding coordination or change issues in operational RFID-based processes. An example would be an anti-counterfeiting monitoring service that analyzes the number of counterfeits over time and locations.

Strategic Layer

Finally, when deploying RFID-based solutions, optimization of processes should yield competitive advantages. Data on the tactical level comprises the information exchange from multiple data sources, and in contrast to the tactical layer, also beyond one's direct supply chain partners. As [7] indicates, strategic information might include point-of-sale information, real-time demand, or trends. All the aforementioned data can be inferred from RFID data traces. Also, the effectiveness of all business operations together with their tactical decisions can be translated into critical success factors (CSF) and aggregated over time and products. This can be useful input for strategic decision-making or long term planning in general. An example would be the mapping of the detected counterfeiting problem to the partner and supplier network to decide about strategic changes in the supply network.

3. Conclusions

We have presented a high-level framework to transform the EPC network into a business collaboration framework. The idea is to standardize common interfaces in the EPC Network also on an inter-organizational level. Organizations can then benefit from a set of applications that become commodities in order to enable high interoperability at low cost. The Service-oriented Architecture (SoA) approach was presented to understand the role and placement of individual network components beyond an operational level. Applications in the described layers are intended to complement the current EPC network architectural framework with existing software suits and completely new applications. We outlined that a categorization between operational, tactical and strategic levels may be useful to clarify the role of future RFID-based applications. Further research is, however, needed to detail our idea and its implementation.

AUTO-ID LABS

References

[1] EPCglobal, "EPCIS 1.0 Specification," 2007, [Online]. Available: http://www.epcglobalinc.org/standards/epcis/EPCIS_1_0-StandardRatified-20070412.pdf

[2] T. Erl, *Service-oriented architecture,* Prentice Hall, 2005.

[3] E. Fleisch, *Das Netzwerkunternehmen,* Springer, Berlin, 2001.

[4] C. A. Hill, and G. D. Scudder, "The use of electronic data interchange for supply chain coordination in the food industry," *Journal of Operations Management*, 20, 2002, pp. 375-387.

[5] *Introducing Information Management: The Business Approach,* Elsevier Butterworth-Heinemann, 2006.

[6] H. L. Lee, and O. Ozer, "Unlocking the value of RFID," *Graduate School of Business, Stanford University, working paper*, 2005,

[7] J. Li et al., "A strategic analysis of inter organizational information sharing," *Decision Support Systems*, 42, 2006, pp. 251-266.

[8] K. Michael, and L. McCathie, "The pros and cons of RFID in supply chain management," 2005, pp. 623-629.

[9] *Security Aspects and Prospective Applications of RFID Systems,* Federal Office for Information Security, Bonn, Germany, 2004.

[10] T. Staake, F. Thiesse, and E. Fleisch, "Extending the EPC network: the potential of RFID in anti-counterfeiting," New York, NY, USA, 2005, ACM Press, pp. 1607–1612.

[11] K. Traub et al., "The EPCglobal Architecture Framework," 2005, [Online]. Available: http://www.epcglobalinc.org/standards/Final-epcglobal-arch-20050701.pdf

[12] S. F. Wamba, L. A. Lefebvre, and E. Lefebvre, "Enabling intelligent B-to-B eCommerce supply chain management using RFID and the EPC network: a case study in the retail industry," *ICEC '06: Proceedings of the 8th international conference on Electronic commerce*, Fredericton, New Brunswick, Canada, 2006, ACM Press, pp. 281–288.