Towards a Business Collaboration Framework for the EPC network

By analyzing the functionality of the EPC network against common mechanisms of business coordination, we identify additional software layers, necessary to transform the EPC network into a business collaboration framework.

Alexander Ilic
ETH Zurich, Switzerland
ailic@ethz.ch

Florian Michahelles
ETH Zurich, Switzerland
fmichahelles@ethz.ch

Introduction

The reason why companies deploy RFID solutions is clearly to improve the efficiency of business processes [4]. With globally unique numbering schemes, such as the Electronic Product Code (EPC) [3], 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 [2], or even the ability to detect counterfeits [6].

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 data and thus enable efficient business collaborations on a global scale. A first step towards that direction is the so-called EPC network architecture [3], which tries to standardize components and interfaces to serve as a basis for RFID-driven business. Currently, only the local components specified in the EPC network architecture are being used [7]. Inter-organizational collaborations on RFID-data exist, but focus on small closed-loop applications [5]. In order to exchange data on the network, organizations are forced to use proprietary software that connects their local EPC network stacks and thereby their businesses. The lack of standardization and high costs for developing common components every time again is hereby a major hindering factor for the adoption of RFID [4].

In this article we analyze the EPC network and identify additional layers necessary to transform the EPC network into a large-scale business collaboration framework.

Network access and enabling layer

In the following we apply a common concept of business coordination [1] to the EPC network and explain how successful inter-organizational integration can be achieved with services and standards. Starting with applicability of existing EPC Network components, we identify which essential network components are still missing. While local standards are sufficient for proprietary closed-loop applications, the following steps reveal the need amendments of existing local data standards. For example while event attributes like “publisher” or “location” may have a defined semantic inside a defined network of companies, they may lead to ambiguities when used in another context.

Step 1: Find partner

In a data-driven architecture, the most challenging goal is to find data providers.

Currently, the Object Naming Service (ONS) provides lookup capabilities to find the initial creator of information associated with a specific object. However, the ONS cannot return information about other data-points, 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 [3], 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.

Business supporting layers

While the previous coordination steps revealed the technical foundation of a semantically integrated infrastructure, the following part highlights business layers that should seamlessly integrate the aforementioned technical infrastructure with business operation processes.

Supporting business operations

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. Usually, these RFID-based services are directly embedded into processes. 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.

Supporting managerial decision making

For an optimal management of RFID-based processes, a layer is needed that allows for assessing the effectiveness of the operations. Data that is generated by the business operations layers can directly be evaluated and compared in a “to be” and “is”. Services in this layer keep track of the performance and monitor operations on a broader scope. As this increases transparency and provides clear output characteristics, managers are supported in their decisions about coordination and 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.

Supporting strategic decision making

Finally, when deploying RFID-based solutions, optimization of processes should yield competitive advantages. We propose therefore a layer that translates the data generated by the managerial decisions and the effectiveness of the business operations into critical success factors (CSF) that can be used to support strategic decision-making. An example would be the mapping of the counterfeiting problem to the partner and supplier network to decide about strategic changes in the business.

Conclusions

We have presented a potential roadmap to transform the EPC network into a business collaboration framework. Additionally, a layer-based taxonomy was presented that provides the basis for a common understanding about the role and placement of individual network components. The layers complement the existing EPC network architecture, with starting at the "Data source" layer that includes services like the EPCIS. The next layer was derived by looking at the generic problem of semantic integration across organizations and is called the "Network access and enabling" layer. The upper three layers depend on the level of business collaboration that a service provides. We outlined the need to distinguish between operational, managerial and strategic decision-making support services.

References

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

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

[3] K, Traub, G, Allgair, and B. H, "The EPCglobal Architecture Framework," *EPCglobal Final Version*, 2005,

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

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

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

[7] 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.

Supporting material

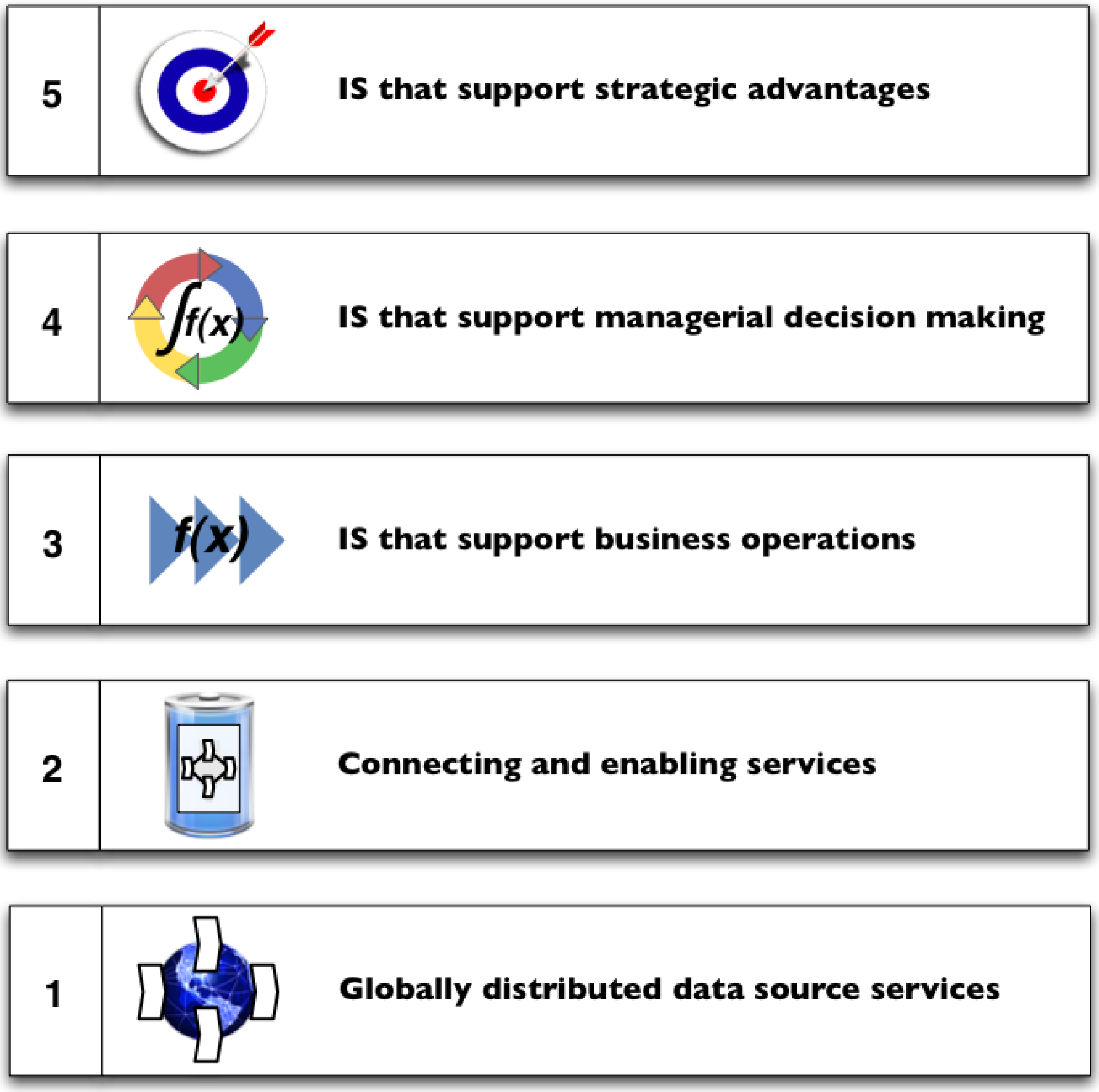
5
IS that support strategic advantages
4
f(x)
IS that support managerial decision making
3
f(x)
IS that support business operations
2
Connecting and enabling services
1
Globally distributed data source services

Figure 1. Proposed layers for business collaboration framework on top of the EPC Network