Discovery Services—Enabling RFID Traceability in EPCglobal Networks

Steve Beier[†] Tyrone Grandison[*] Karin Kailing[*] Ralf Rantzau[†]

[*]IBM Almaden Research Center
650 Harry Road, San Jose, CA 95120, USA
{tyroneg, kkailin}@us.ibm.com

[†]IBM Silicon Valley Laboratory
555 Bailey Ave, San Jose, CA 95141, USA
{sbeier, rrantza}@us.ibm.com

Abstract

The EPCglobal consortium defines standards to enable data sharing of electronic product code related information within and between enterprises, which typically comprises events of RFID readers as well as product information about the tagged products. An EPCglobal network consists of nodes, each of which may have complex data usage and sharing policies and have a need to collaborate in order to extract full value from the network. The Discovery Services is the key step in enabling creation and adoption of this network of possibly heterogeneous enterprise systems.

This work focuses on providing a first implementation of a simple, scalable infrastructure for building Discovery Services. The demonstration illustrates the interplay of three elements of an EPCglobal network: Discovery Services, EPC Information Services (EPCIS), and an application that uses Discovery Services to query EPCIS, which are hosted on multiple EPCIS servers. The application tracks the freshness of avocados across a food supply chain and allows the rerouting of products that are unsatisfactory. The standardization of Discovery Services by EPCglobal is still pending.

1 Introduction

With initiatives like the electronic product code (EPC) and upcoming technologies like RFID, new traceability applications emerge everywhere. Parties that want to share their data to create business value need the right technology. New mechanisms to query traceable data are needed to give companies incentives to participate in global EPC data networks. Apart from business considerations, they will share their data only if the services infrastructure, such as the EPCglobal Network architecture, is scalable, secure, and easy to use.

The EPCglobal Network architecture describes components and interfaces for the EPC-related information interchange between servers that contain information related to items identified by EPC numbers [2, 3, 1]. The servers (EPCISes), which are linked via a set of network services, store relevant information related to specific EPC numbers of their products. Each EPCIS contains the read time (at the reader), capture time (at the EPCIS), reader location, action (typically, *observe*), and several optional attributes of all the EPCs of interest. The event schema can be extended by additional, company-specific fields. For example, a reader may also capture the temperature or radioactivity of an item. The EPCIS provides an interface for executing ad-hoc queries as well as standing queries that deliver new results periodically. The standardization of this interface encourages the marketplace to provide vendor-specific implementations, which increase the scope of use of the EPCglobal network services.

Many of the most valuable use cases for RFID require information exchange between companies, but gathering cross-company supply chain data can be expensive, time consuming and unrealizable given security concerns. Properly designed Discovery Services can be used to address these issues.

2 Discovery Services and EPCglobal Networks

Discovery Services simplify the data exchange process by offering a service that links information about RFID-enabled products as they move through the supply chain. The addition of Discovery Services to the EPCglobal Network offers trading partners the ability to find all parties who had possession of a given product and to share RFID events about that product. This network allows participants to pro-actively manage their supply chains and ultimately to realize more of the benefits that RFID promises.

EPCglobal proposed an Object Name Service as an instantiation of Discovery Services [4]. The proposal is based on the idea that like the Domain Name Service for the Internet, the EPCglobal network would need an Object Name Service. EPCglobal suggested to simply encode an EPC number in a syntactically correct domain name and to use the existing DNS infrastructure to retrieve a list of all EPCIS that store information

International Conference on Management of Data
COMAD 2006, Delhi, India, December 14–16, 2006

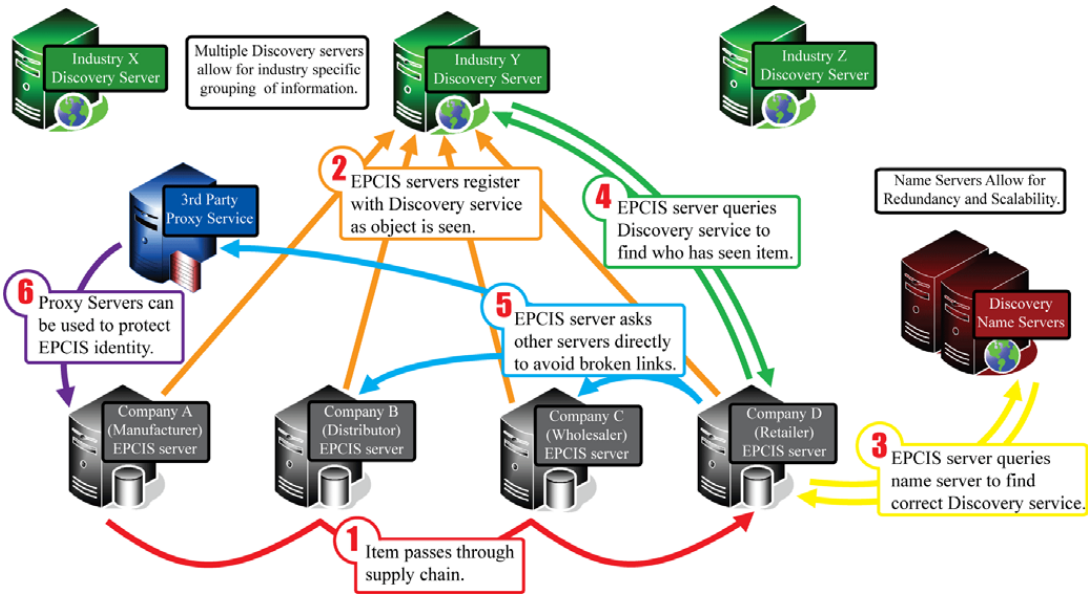


Figure 1: Architecture of an EPCglobal network

about the respective EPC number. However, unlike the Internet where domain addresses are freely available to everyone, EPC-related information needs to be protected and will only be shared selectively. A security analysis [5] of the Object Name Service proposal shows that the Domain Name System is not a good fit for building Discovery Services.

In the following, we present an approach to achieve the same functionality as the Object Name Service by using different technology. It is assumed that before a company in the supply chain is able to use the Discovery Services, the company will need to be authorized by the authoritative party (e.g., EPCglobal). After registration, a trusted third party (e.g., VeriSign) will deliver a signed certificate to the company that has been authorized. This certificate is used in all transactions with the Discovery Services.

Discovery Services are composed of a database and a set of web service interfaces. When these interfaces are exposed to the Internet, they can be invoked by any computer on the Internet but the authorization described above is used to limit read or write access to certain data elements and a permanent log of transactions is also made. These web service interfaces will allow an authorized company to register EPCs and EPCIS URL links when they manufacture or receive a new product. Additionally, authorized companies may be allowed to retrieve links to all EPCIS servers that contain events for a specific EPC. Discovery Services store records with the following attributes:

- *EPC* number of the item,
- *URL* of the EPCIS that submitted this record to indicate that it had custody of the item,
- *certificate* of the company whose EPCIS submitted this record,
- *visibility*, a flag indicating if this record can be shared with anybody or only with parties who submitted records about the same EPC, i.e., supply chain partners, and
- *timestamp* when this record was inserted.

The architecture of an EPCIS network is sketched in Figure 1. At the bottom, there are several EPCIS servers, typically one per supply chain partner. At the top, there are one or more Discovery Services instances, typically each serving a separate type of industry. While an item passes through the supply chain—see number (1) in the figure—an EPCIS registers the EPC with its Discovery Services (2). This happens only when the EPCIS captures an event about the EPC for the first time. By registering the EPC with the Discovery Services, the EPCIS declares that it had custody of the item associated with the EPC and is thus a keeper of information about the item.

The figure also illustrates the case where company *D*, a retailer within a supply chain, searches for information about a product with a given EPC it has received. It has to find the EPCIS of all companies that have had custody of the item. Unless, the EPCIS of company *D* does not already have the address of its Discovery Services, it looks it up at a Discovery Names Server (3), which is an optional element of the EPCglobal network. It calls a Discovery Services web service to retrieve the URLs of EPCIS that have seen the given EPC (4). The EPCIS of company *D* then queries the EPCIS using the URLs returned by Discovery Services through EPCglobal web services (5). Some of the URLs may not point to a company's EPCIS directly because these companies decided to anonymize their address using (third-party) proxy servers, which are optional elements that are transparent to the EPCglobal network.

3 Privacy and Security

EPC event data are valuable assets that a company is likely to share only with certain trading partners and only under special conditions. There is no specific security or privacy framework suggested by the EPCglobal standard. We propose the following safeguards for the EPCglobal Network architecture:

- EPCIS: Role-based, policy-based, cell-level data disclosure control [6]. The owner of an EPCIS has to be able to restrict data disclosure to the parties that have a business reason to access the information. Typically, these are the trading partners in the supply chain (or other parties that "pay" for the information). While some parties such as shipping companies may need to see product-specific attributes like temperature for product quality control, others such as a retailers should only be able to see quantity information like the number of avocado crates in a container.

- Discovery Services: Row-level data access control. The owner of a record decides whether the record can be shared with anybody or if access is restricted to parties that own records for the same EPC number (i.e., they belong to a chain of trading partners). Further, group-based access control would be possible as well, but we did not realize this idea, and it would require a concept to manage the group information.

- Internet: Proxy servers can provide a level of anonymity to entities interacting in an EPCglobal network (see item 6 in Figure 1).

4 The Demo

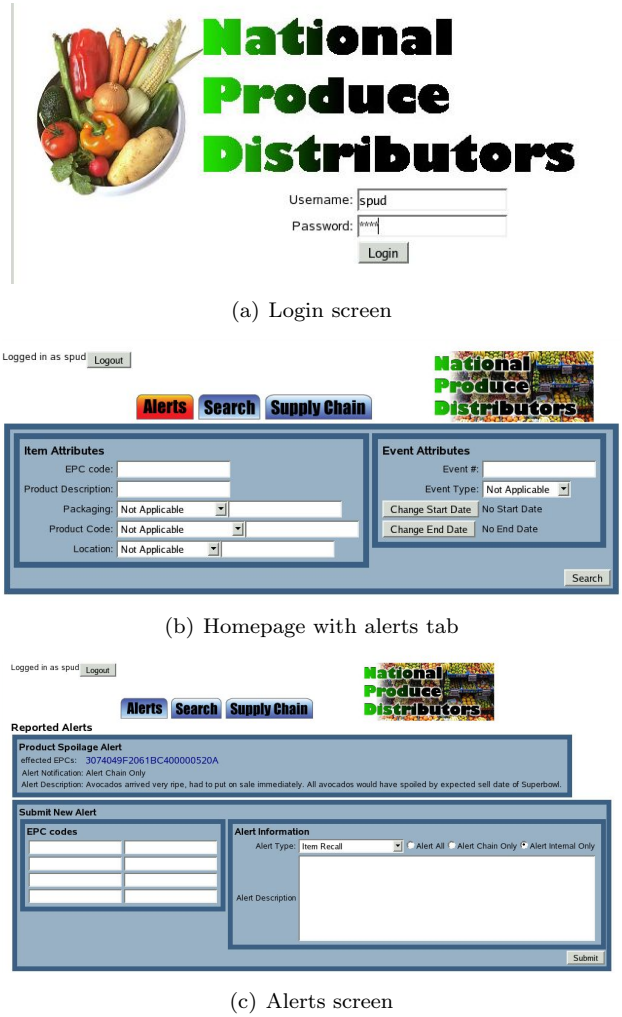
This demonstration shows an application (hereafter called *eManage*), which leverages EPCIS and the Discovery Services.

4.1 Scenario

It is one week before Super Bowl, the championship game of the National Football League in the United States and a nation-wide television highlight. Preparing a home-made guacamole from California-grown avocados for this event has become very popular. *National Produce Distributors (NPD)*, a U.S.-wide fruits and vegetables wholesaler supplies many retailers, among them the *Trader Jill's (TJ)* store chain that are currently filling their avocado stocks. Spud is an NPD supply chain manager, Sandy is a TJ's store manager in San Fernando, California, and Nick is a TJ's store manager in New York City. Both, Sandy and Nick are expecting shipments of fresh California-grown avocados. (The companies are fictitious.)

4.2 Architecture

The system architecture of the EPCIS network realized in the demo encompasses the following components:



(a) Login screen

(b) Homepage with alerts tab

(c) Alerts screen

Figure 2: Demo screenshots

- Discovery Services (one instance),
- EPCIS (several instances), and
- application eManage (one instance).

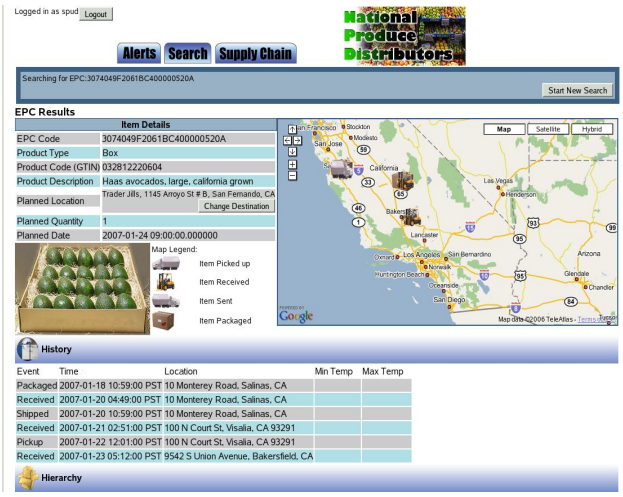
4.3 User Interface

The scenario is realized in our demo by user interactions with the following graphical interfaces:

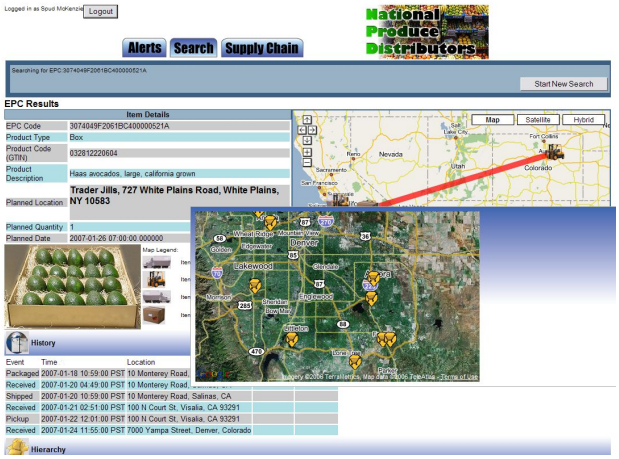
Login screen: Spud logs into eManage using a web browser to access the product tracking application using his user name and password (see Figure 2(a)).

Query screen: eManage displays a home page (Figure 2(b)). He notices that the *alerts* tab is red and clicks on it.

Alert screen: He sees an alert from Sandy stating that the avocados she received were already very ripe (Figure 2(c)). He clicks on the EPC link of



(a) EPC details screen



(b) Container details screen

Figure 3: More demo screenshots

the referenced avocado crate to see detailed information.

EPC details screen: He does not notice anything out of the ordinary on the EPC details screen (Figure 3(a)). He clicks onto the container EPC to see what happened to Sandy's shipment on a higher item aggregation level.

Container details screen: On the container details screen (Figure 3(b)) he notices that the temperature on the container during one of the transport legs was above the optimal temperature. This is why that the avocados had ripened more quickly than expected. By drilling into different EPC codes (using Discovery Services in the background), Spud also notices that the time and location for the crates deliveries is several days away. He worries that the avocados will be too ripe by the time that they arrive. Spud finds out that some crates are intended to be sent to Nick and will arrive in 3 days from now.

EPC location map: He reviews the map that is displayed at the bottom of the page. It shows that some crates are currently in Colorado and he tries to proactively re-route them to local stores in Colorado by clicking on the store icons on the map. He also adds a note to all of the affected locations so that other users of the system will know why the product has been rerouted.

5 Conclusion

Commercial enterprises are moving towards a world of item-level tagged products, where the EPCglobal standards will drive the labeling mechanism, the transmission protocol and the network formation. However, as information is the most valuable corporate asset and possibly competing companies may inadvertently create EPCglobal networks, the key enabler for deriving maximal value from this advance is a scalable, security- and privacy-aware Discovery Services that enable selective information sharing and proactive product management. Discovery Services are as crucial to an EPCglobal network as the Domain Name Service is to the Internet. In this demo, we provide the first ever implementation of Discovery Services and showcase their feasibility and usefulness. We show a scalable architecture where the load can be balanced between multiple Discovery Servers and highlight some features to ensure privacy and security (use of certificates, enforcement of row-level data access control, incorporation of proxy servers). The current implementation is relatively simple, however it was designed with extensibility in mind.

Acknowledgments

Thank you, Mark Bailey, Jeff Chen, Paul Nepywoda, and Tracy Olsen, for putting the Discovery Services and the demo into reality.

References

[1] S. S. Chawathe, V. Krishnamurthy, S. Ramachandran, and S. E. Sarma. Managing RFID data. In *VLDB*, pages 1189–1195, 2004.

[2] EPCglobal. *The EPCglobal architecture framework, final version*, July 1, 2005.

[3] EPCglobal. *EPC Information Services (EPCIS) Version 1.0 Specification, working draft*, June 8, 2006.

[4] EPCglobal. *Object Naming Service (ONS) Version 1.0, ratified version*, October 4, 2005.

[5] B. Fabian, O. Günther, and S. Spiekermann. Security analysis of the Object Name Service for RFID. In *Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing*, 2005.

[6] K. LeFevre, R. Agrawal, V. Ercegovac, R. Ramakrishnan, Y. Xu, and D. J. DeWitt. Limiting disclosure in Hippocratic databases. In *VLDB*, pages 108–119, 2004.