Dual Ownership: Access Management for Shared Item Information in RFID-enabled Supply Chains

Alexander Ilic, Florian Michahelles, Elgar Fleisch
Information Management, ETH Zurich, CH-8092 Zurich, Switzerland
{ailic,fmichahelles,efleisch}@ethz.ch

Abstract

RFID tags combined with globally unique numbering schemes such as the Electronic Product Code (EPC) help standardizing the communication along the supply chain. Participants generate and share item information to collectively build digital lifecycle records. Yet, the challenge of efficient access management for item-level information still remains open. This paper introduces a novel concept for data access management, called Dual Ownership. The model grants access control to parties that can prove the physical possession of an item. RFID technology hereby tracks the transitions of physical possession to translate them to data access permissions. This paper describes the concept of Dual Ownership and discusses its implications.

1. Introduction

In supply chains, information sharing can improve economic performance dramatically by reducing uncertainty [1]. The supply chain is more responsive to changing conditions and can be coordinated more efficiently. Analytical and numerical analysis indicate that sharing of shipping quantities and inventory levels can lead to reduced stock levels and reduced costs already in a two-level supply chain [2]. The benefits of information sharing are even greater in large supply chains that take advantage of the economies of scale with respect to the value of information [3].

The prerequisite for unleashing the potential of information sharing is accurate data gathering. Due to RFID technology, data gathering is now possible on an item-level granularity at low costs [4]. Globally unique numbering schemes such as the Electronic Product Code (EPC) [5] standardize hereby a common point of reference. Item data can be aligned to this reference to build a digital lifecycle record for each item. Accordingly, centralized information systems can store static and dynamic properties of items such as quantity, current location and history data. However, as these data records are connected to business processes, there is a strong need for restricting access control. Depending on these processes, this data should be made available to organizations downstream or upstream the supply chain. At each echelon of the supply chain, an organization should be able to decide what data should be shared with whom. Traditional access management concepts are limited to scenarios where organizations remain in control over items. However, due to the trend of moving from pallet, to case, to item-level granularity, the complexity of managing the object associated data increases. Individual items are shipped to different parties and allocated on demand. The number of parties, data records of items, their mutual allocation and the assignment of access permissions complicate the situation. For managing these transitions, static access control models are no longer sufficient. Additional effort is required to continuously adapt the sharing access to resemble the situation of the real world.

This paper introduces a novel concept referred to as Dual Ownership. This concept proposes to link physical flow of goods with access control in information systems. Section 2 gives a brief overview of related work, section 3 describes Dual Ownership, and section 4 introduces read access delegation as an extension to the model. Finally, section 5 sketches a sample scenario and section 6 concludes the paper with a short discussion of the implications of Dual Ownership.

2. Related work

Access control models are key concepts for information technology security. However, when used in the context of information sharing, Access Control Lists (ACLs), Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-based access Control (RBAC) fall short in terms of

scalability [6]. Their main application domain is across small company networks or within an enterprise. Literature that covers the problem of access management and security control between organizations can be found in the area of Virtual Enterprises. Virtual enterprises are networks of independent organizations that cooperate by sharing resources across enterprises to be able to rapidly respond to customer expectations [7]. Secure information sharing is one of the key factors for their success. The access models in this domain are designed to work across organizational boundaries. Unfortunately, the approaches assume a determined participant base which is directly or indirectly associated with determined resources [6][7]. Managing item-level permissions with these approaches requires big efforts in updating item allocations, participant lists and their relationships [8]. The process must continuously update access according to a changing context. Innovative ways to manage access control by utilizing the context itself can be found in the area of pervasive computing. As the subject of interest is the exchange of item related information, object-oriented [9], context deductive [10] and token-based models [11] were examined. Yet, the stated literature does not cover inter-organizational aspects for trust management and needs complementing models to be adaptable to the business context of goods.

In the following section, the Dual Ownership model bridges the outlined gap between pervasive computing and virtual enterprises: item-level context is combined with the cross organizational flow of goods.

3. Dual Ownership Model

The flow of goods between organizations (Figure 1) consists of a number of property right transitions from one owner to the next one. For the transitions, a certain level of trust and proper handling is ensured. They base on established relationships, common agreements or contracts. The idea of the Dual Ownership model is to utilize these already existing relationships to align the access control of an information system accordingly.

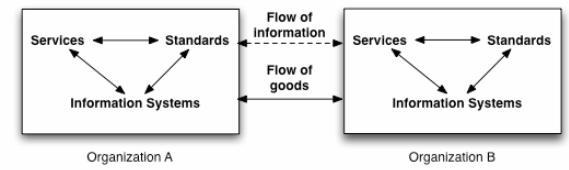

Figure 1. The flow of goods is properly managed. However, the flow of information is managed separately from this.

The key principles of Dual Ownership are:

- (P1) Power of control bases on physical possession
- (P2) Handing over physical control implies handing over access control

The Dual Ownership principles resemble approaches that are well known from our daily life. For example, when lending a car to a friend, we explicitly hand over the key (P2) so that the friend is able to drive the car (P1). The key is the proof of current ownership of the car and enables the use of the car.

3.1. Implications of principle P1

Applied to an information system world, P1 requires a similar concept to prove the item ownership. Only then, the information system enables the owner to control access for its data record. The concept for proving ownership is called the Dual Ownership Link (Figure 2). It connects physical items with their data record. The link remains established until the next owner establishes a link. Only with an established link, a party is able to find, read or contribute data to a corresponding item record.

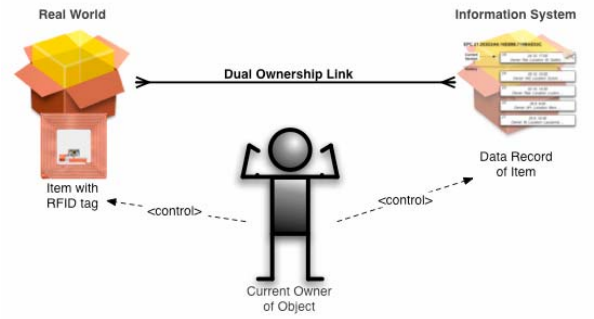

Figure 2. Dual ownership is a combination of both, item-related power of control in the physical world and in the information system.

The proof of ownership includes the fulfillment of the following three requirements:

- Proof identity of item (e.g. EPC number)
- Proof identity of owner
- Proof timeliness of above ones

3.2. Implications of principle P2

The principle P2 of the Dual Ownership model demands a concept for handling past, present and future access to item records after ownership changes. To illustrate this concept, a sample scenario is presented. The scenario shows how an item from

Manufacturer M is shipped by a logistics provider L to a wholesaler W. Every party is participating in a shared information space that contains the data record of the item.

Each time an item is scanned the current owner (authorized through the Dual Ownership link) contributes event data to the shared item record. Figure 3 shows the item record after the item reached W. All contributed events are in chronological order. For convenience, each record is versioned from V1 to V4. The current version V4 reflects the most recent status of the item. V1 till V3 are referenced as history data and were valid at the specified time. For transparency reasons, a party can retain read access to information that was valid during its ownership. In the example, M can still access V1 even if there is a more up to date version. The most recent version is restricted to access by the current owner.

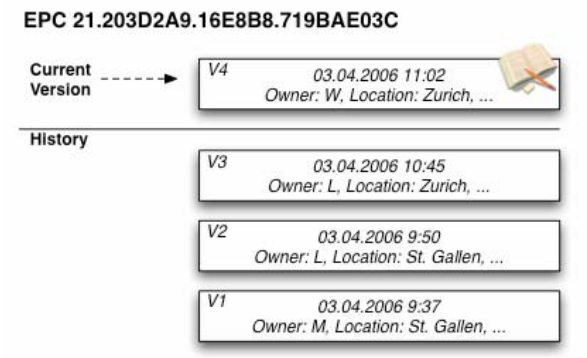

Figure 3. An example of an item location history consisting of several item event records added by different partners.

Beyond access to single data records, search queries are very important. Information systems provide query interfaces to extract relevant information out of masses of data records. Search permissions fall into the category of read access. A search service generally indexes all available records and provides a query interface to retrieve specific results. According to the Dual Ownership model, the search space must be restricted. Only users with established Dual Ownership links can execute queries upon most recent data records. Otherwise, previous owners would be able to retrieve future data beyond their item possession.

4. Upstream and downstream information sharing

The basic Dual Ownership model covers sharing of information by directly following the physical flow of goods. For business applications like track & trace or Vendor Managed Inventory (VMI) this is not sufficient. These applications require also upstream and downstream information sharing with remote parties. Upstream information sharing refers to providing access to the current item record for a remote party that formerly possessed the item. Downstream information sharing covers granting of access permissions to current item records to remote parties that were not in possession of the item before.

The Dual Ownership model is extended so that an owner can delegate read access to remote parties. In contrast to normal read permissions, remote access does not require a Dual Ownership link. Instead, the access is tied to the identity of the remote party. Accordingly, the search space includes only accessible records of the party (Figure 4).

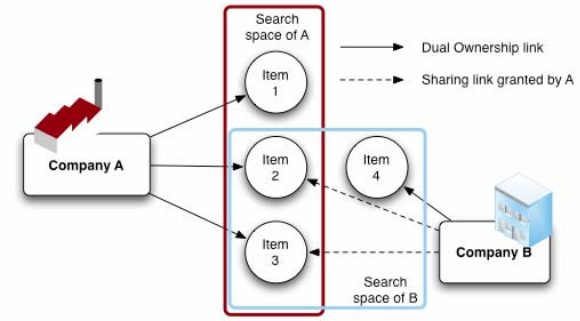

Figure 4. Dual Ownership requires individual search spaces based on physical possession and granted access by other (item) owners.

For example, moving outbound products to a certain pick area triggers a certain policy rule. When passing the RFID gates of the area, the data records of the items are automatically shared with the appropriate logistics provider. By querying the database, the logistics provider can see quantity, type, and other properties of the products in the pick area.

As long as a party is in physical control of an item, it may control read access for remote parties. With a change of ownership, all granted sharing permissions expire. If read access to most recent records should be retained over ownership changes, the next owners must explicitly specify this in their sharing policy.

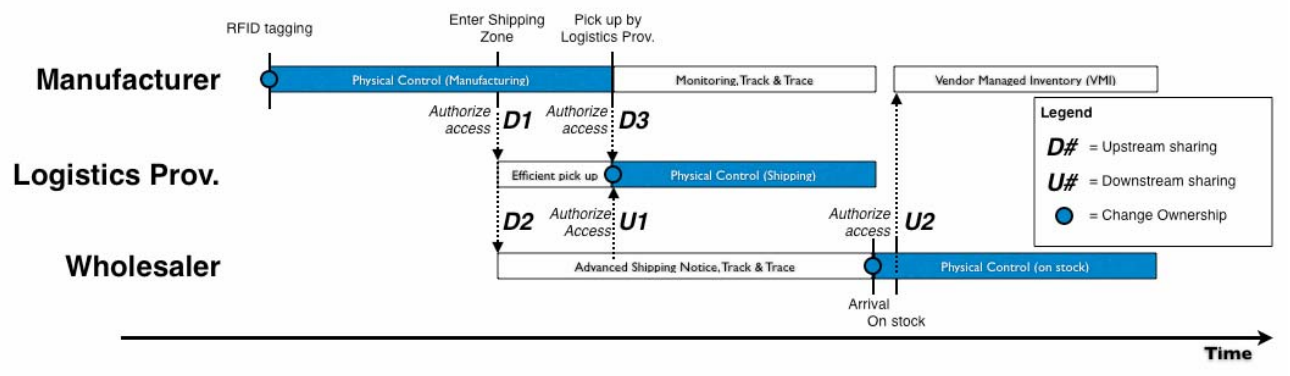

Figure 6. The shaded bars indicate phases where an owner controls item-related data. During these phases, an owner can grant upstream or downstream sharing access to other parties. The white bars represent applications that rely on information sharing.

5. Sample scenario

To illustrate the presented concepts the flow of an item from manufacturer to wholesaler is described (Figure 5). Business applications like track and trace, efficient pick up and Vendor Managed Inventory motivate hereby the sharing of information.

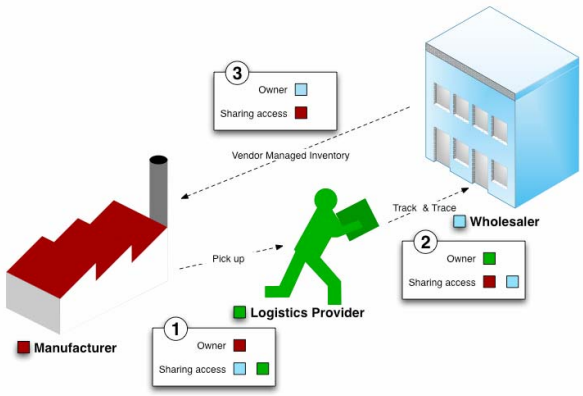

Figure 5. A business scenario showing the flow of an item from the manufacturer to the wholesaler. The boxes indicate the sharing policies of the owners.

A logistics provider carries out the transportation from manufacturer to wholesaler. As items arrive at a party an initial arrival scan of the RFID tags establishes the Dual Ownership links. The predefined permission granting policies shall ensure track and trace for the transportation from manufacturer to wholesaler. As items are on stock at the wholesaler, the manufacturer should be able to execute remote inventory queries. Figure 6 shows the associated sharing relationships in detail. The following section describes the dynamics of the sharing relationships according to the figure.

Whenever an item within the factory of the manufacturer passes the RFID-gates of the shipping zone, the efficient pick up process starts. The final destination, the wholesaler, and the logistics provider automatically get access to the data record. The logistics provider can execute queries to find out what items reside inside the shipping zone and thus determine which of them are ready for pick up. With this information, the logistics provider can optimize the pick up process. Once the items are loaded onto the transporter, policies of the logistics provider become effective. From this point on, manufacturer and wholesaler are granted the permission to execute track and trace queries. On arrival at the final destination, the Dual Ownership link of the wholesaler is established. This automatically transfers control from logistics provider to wholesaler. Finally, when the items are put on stock, sharing permissions are adjusted to enable Vendor Managed Inventory (VMI) for the manufacturer.

This example illustrated how the Dual Ownership model can be applied in a real world scenario. The next section will discuss the effects of Dual Ownership on security.

6. Discussion

Dual Ownership itself can increase the security of information sharing along the supply chain. Its selective access management enables confidentiality between partners. Every organization is in full control of their sharing relationships. With every change of ownership, previously associated permissions are automatically revoked. This reduces the maintenance effort and increases security. Unwarily maintained access permissions cannot affect the next owner. For all items of a current owner, the same company-wide

policy applies. This increases transparency dramatically. Existing contracts and agreements for the flow of goods ensure trust and proper handling between the parties.

Further more threats of injecting false information are mitigated. The risk is reduced from a global to a local context. Only owners of items may contribute new data records. To protect the history of events, previously submitted data cannot be changed. False information can therefore be tracked down to a specific identity. Every access leaves at least the fingerprint with the parameters of identity and time. With this data a security-monitoring tool can be built. A flexible identity management concept must ensure that digital identities can easily be issued and verified. Anonymous access to shared data is not allowed in this model. Every supply chain participant must have an own digital identity.

7. Conclusion and Future Work

Currently there is no access management model for sharing item-level information on a global scale. Recent models are designed for small environments and lack scalability. The presented model shows how business workflows can be utilized to manage access control in information systems. Organizations are identified as valid sources for data contribution by establishing Dual Ownership links. Data records are tied to physical items. The records can be shared in a flexible way. Each organization can have individual sharing permissions with their partners. The automatic clean up on ownership change ensures that previous permission sets have no impact on the next owner. Reduced maintenance and increased transparency make the presented model suitable for a global scale.

Next steps include the further evaluation of benefits and key scenarios. A simulation should investigate the performance of the model and demonstrate the scalability. In order to prove the technical feasibility, a prototype will be developed. It outlines design specific issues and illustrates how the proof of ownership can be conducted in practice.

Future research directions may include ways to further improve resource and information integration among organizations. But also the consumer environment can benefit from the Dual Ownership model. For example, the concept of upstream and downstream information sharing can be potentially adapted to achieve a high level of privacy by letting smart items only talk to partners that the current owner allows to.

8. References

[1] F. Sahin, and J. Robinson, E. Powell, "Information sharing and coordination in make-to-order supply chains," *Journal of Operations Management*, 23, 2005, pp. 579-598.

[2] H.L, Lee, K.C, So, and T. C.S., "The Value of Information Sharing in a Two-Level Supply Chain," *Management Science*, 46, 2000, INFORMS, pp. 626–643.

[3] B, Huang, and I. S.M.R., "Production Control Policies in Supply Chains with Selective-Information Sharing," *Operations Research*, 53, 2005, pp. 662–674.

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

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

[6] T.-Y. Chen et al., "Development of an access control model, system architecture and approaches for resource sharing in virtual enterprise," *Computers in Industry*, In Press, Corrected Proof, 2006,

[7] H, Afsarmanesh, C, Garita, and H. L.O., "Virtual Enterprises and Federated Information Sharing," *Proc. of the 9th Int. Conf. Database and Expert Systems Applications (DEXA 1998)*, 1998, Springer, pp. 374–383.

[8] I, Foster, C, Kesselman, and T. S., "The Anatomy of the Grid: Enabling Scalable Virtual Organizations," *International Journal of High Performance Computing Applications*, 15, 2001, pp. 200–222.

[9] C. Yang, and C. N. Zhang, "An approach to secure information flow on Object Oriented Role-based Access Control model," *SAC '03: Proceedings of the 2003 ACM symposium on Applied computing*, 2003, ACM Press, pp. 302–306.

[10] U. Hengartner, and P. Steenkiste, "Exploiting information relationships for access control in pervasive computing," *Pervasive and Mobile Computing*, 2, 2006, pp. 344-367.

[11] L.E, Holmquist, J, Redstroem, and L. P., "Token-Based Access to Digital Information," *Proceedings of First International Symposium on Handheld and Ubiquitous Computing (HUC'99)*, 1999, Springer, pp. 234–245.