The Dual Ownership Model: Using Organizational Relationships for Access Control in Safety Supply Chains

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

Abstract

Counterfeits and contaminated drugs are recognized as a threat to consumer safety. To fight counterfeiting and protect consumers, public health institutions such as the US FDA demand organizations to electronically document the pedigrees of prescription drugs [3]. As the documentation process involves joint collaborations of multiple organizations along the supply chain on electronic pedigrees for billions of individual goods, new and scalable access control models are needed. Therefore, this paper presents a novel concept, which leverages existing organizational relationships to manage access control based on physical possession. The concept is evaluated against other existing models and discussed.

1. Introduction

According to a recent fact sheet of the WHO, counterfeit drugs are estimated to account for more than 10% of the global medicines market [2]. Counterfeits apply to both, branded and generic products. Mostly, patient safety is endangered due to wrong, insufficient, or inactive ingredients.

To increase patient safety, institutions such as the US FDA require all organizations involved in the distribution and production of prescription drugs to document the chain of custody of individual products [3]. This documentation process forms the so-called electronic pedigree. Each organization within the supply chain extends the pedigree record with its arrival or shipment data. As each party digitally signs and adds data, a complete pedigree of the product is established. At the point-of-sale, the FDA requires pharmacies to conduct an integrity verification of the electronic pedigree. This process guarantees that each pharmaceutical product is subject to high quality, safety, and efficacy standards for production and distribution.

Radio Frequency Identification (RFID) technology and globally unique numbering schemes such as the Electronic Product Code (EPC) [11] enable standardized communication along supply chains. The attachment of RFID tags to individual products allows for gathering item-level events at low cost. By sharing and integrating these events, a consistent electronic pedigree can be built. The US FDA recognizes that "electronic track and trace technology, including radio frequency identification (RFID), would provide an electronic safety net" [3] for delivering end-to-end patient safety.

However, organizations are reluctant to share data of item-level granularity, because this information can be misused to reveal strategic information. For example, by correlating the events with business process data, production or sales figures can be derived. For that reason, emphasis needs to be put on the security aspect of information sharing. Consequently, the underlying data sharing model must cope with the complexity of managing access permissions for millions of individual drug packages. Particularly, access control electronic pedigrees must be transferred to parties that receive the physical goods.

The aim of this paper is to introduce a novel model, called Dual Ownership, to simplify these access control transitions for safety applications. Instead of continuously remodeling access control into information systems, the model links access to item-level pedigree data to physical possession of an item: whoever can prove the control over the physical item is granted access rights for the associated pedigree. This paper is structured as follows. Section 2 gives an overview about information sharing models in general and highlights the problem of access control transfer. Section 3 investigates related work and outlines that current access models alone are not able to scale well on an inter-organizational context. Section 4 motivates the idea for Dual Ownership and introduces the concept. In Section 5, Dual Ownership is applied to the

electronic pedigree application. An interaction complexity comparison is given to compare Dual Ownership with other important architectures. The results of this paper are discussed in Section 6 followed by final conclusions in Section 7.

2. Background

The electronic pedigree service is an information sharing application. Information sharing models describe how information of an organization A can be made available to an organization B. Inseparably tied to the question of information transfer, is the challenge of access transfer. In order to tackle this challenge, the background of information sharing must be understood. According to the categorization of Lee [6], there are three different models for information sharing in supply chains, namely the information transfer model, the information hub model and the third-party model. As the third-party model is a variant of the information hub model [6] (with differences that are not relevant for this paper) the following sections will focus on the first two categories.

2.1. Information transfer model

In the information transfer model, the shared data is extended by each party locally and then completely transferred to the next party [6]. Access control is hereby mostly tied to the shared information assets. A recipient can extend or transfer the information asset. Interfaces for incoming or outgoing information take care of authorization, integration and transfer of shared data. The mode of information sharing is a costly 1:1 relationship. Every participant in such a supply chain application must accept and then transfer the information to the next partner. Otherwise the entire information flow could be blocked at one point.

2.2. Information hub model

The second approach is a centralized approach that is called information hub model [6]. The shared data is stored within one logical information system. Each authorized party can contribute service-related data to the central information hub. To be authorized to submit information, access control must be transferred from one authorized party to the new one. The organization that is currently in control must grant appropriate access rights to the next partner. Instead of costly 1:1 relationships, the information hub model enables information sharing at low-cost. In contrast to the information transfer model, the setup costs for each participant are low.

3. Related work

In information hub models, many organizations share data through a single information system. The success of such a system heavily depends on a secure and scalable model to transfer access control from one legitimate party to another. While traditional access control models are a key concept for information technology security in general, their applicability for information sharing must be carefully investigated. For example, when used in the context of the information hub model, Access Control Lists (ACLs), Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-based access Control (RBAC) fall short in terms of scalability [1]. 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 [5]. 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. However, these approaches assume a determined participant base which is directly or indirectly associated with determined resources [1][5]. Managing item-level permissions with these approaches requires significant efforts in updating item allocations, participant lists and their relationships [9]. The process must continuously update access permissions 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 [13], context deductive [8] and token-based models [12] 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.

To conclude, current access models alone are not sufficient to enable inter-organization information sharing. The outlined gap demands for scalable concepts to simplify access management transitions on inter-organizational contexts.

4. Dual Ownership

In the following section, the Dual Ownership model bridges the outlined gap between pervasive computing

and virtual enterprises to simplify access management in an information hub model.

4.1. Utilizing existing relationships

Globalization and the concentration on core competencies lead to more complex supply chains and dynamic relationships. The relationship networks between partners are hereby actively managed and optimized. Laws, contracts, incentives or strategic dependencies ensure that the relationships are trustworthy enough to form a basis for business transactions. One particular part is the logistics network, which ensures the proper flow of goods between suppliers and customers. Within the network, each shipping item may take individual routes. In parallel, each item may have associated digital data records, which should be shared with the next partners in the logistics path. Figure 1 gives an example of a logistic path that an item may take from manufacturer to retailer. By generating and collating event information on the way an individual electronic pedigree can be formed. The challenging question of who is authorized to append and access event data can be delegated to the flow of physical goods: only the party in possession of an item can access or extend its pedigree. Hence, the transfer of access control from one party to the other becomes the key challenge.

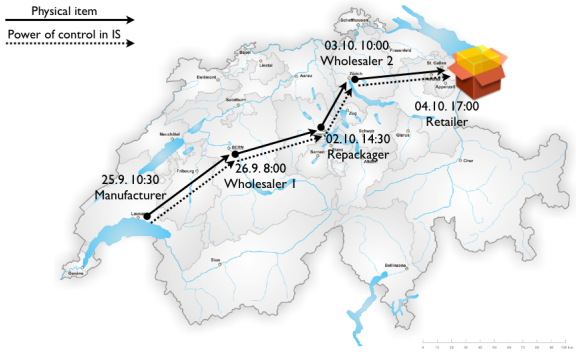

Figure 1. Path from manufacturer to retailer

As outlined, the flow of goods between organizations consists of a number of property right transitions from one owner to the next one. The idea of the Dual Ownership model is to utilize these already existing relationships to align the access control of an information system accordingly. 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 everyday practice. 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 usage of the car.

4.1.1. Implications of principle P1

Applied to information systems, P1 requires a similar concept to prove the ownership of an item. 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 has the power of control within the information system. An information system may for example associate the right of control with ability to find, read, or add specific data to a corresponding information asset.

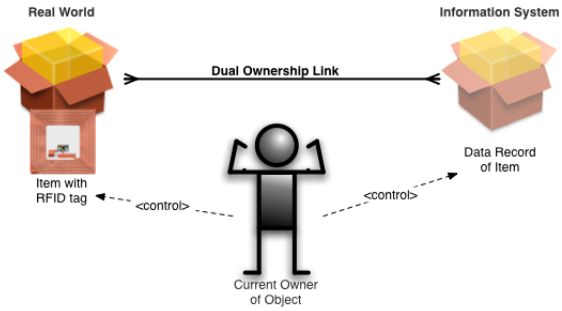

Figure 2. Dual ownership principle

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

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

Defining the extent of control for a certain information system, is up to the service developer and certainly dependent on the specific application. We divide power of control into three categories: read access, write access and delegate access to third parties. Read access refers to the permissions of accessing certain parts or the entire information asset that is connected with the physical item. Write access refers to the permission of contributing statements about items that can only be made truthfully when possessing an item (e.g. location). Delegate access

means the ability of owners to grant or revoke permissions to external parties for the duration of their possession.

4.1.2. Implications of principle P2

By passing one item to the next partner, organizations implicitly agree that their contributed data is now part of the item. The recipient of the item gets the dual ownership of both, the item and the information asset it is connected to. Accordingly, the previous owner cannot withdraw or modify information anymore. At first glance, this may indicate that organizations lose control over their data. Instead, information access is tied to the physical flow of goods, which is clearly defined and managed. In a strongly manufacturer-controlled supply chain, the manufacturer may demand every partner downstream in the supply chain to grant him back the permission to access the information. With these agreements, a manufacturer can get in fact more visibility and control over the supply chain. Also the fact that information of previous owners cannot be withdrawn or modified ensures data integrity and consistency. This fact fits with the behavior of organizations that only share information if the data treatment policy is clearly defined.

4.2. Design considerations

The most important element to implement Dual Ownership is the actual proof of ownership. The proof of ownership is different from sole item authentication. Item authentication aims to provide authenticity of a tag and privacy for its user, which relates to a secure communication channel [10]. In addition, a proof of ownership focuses on the physical association of an authenticated user with an item. To our best knowledge, there is currently just one protocol for RFID systems that addresses the problem of ownership proof and transferal [4]. Even though their protocol focuses on privacy protection, it can probably be extended to serve for a proof of physical possession. In the following we want to provide a simple idea how to achieve a reasonable proof of ownership with a synchronized secret approach. In the synchronized secret approach, tag and back-end continuously and securely update a secret according to a predefined procedure. For every proof a unique combination of user id, item identifier and the current secret on the tag is needed.

5. Evaluation

Based on the functional loop of the electronic pedigree application [7], the interaction costs of the solution are evaluated and compared to other architectures based on the models of Section 2.

5.1. Functional loop

As already stated in Section 1 an Electronic Pedigree service tracks all changes of locations and ownerships of individual items. Figure 3 shows the overall process loop [7] that is executed as drug items travel through the supply chain. The following sections will describe the process steps in detail.

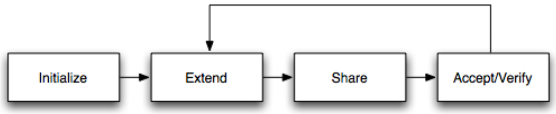

Figure 3. Electronic pedigree process

Initialize: The process step initialize usually takes place at the manufacturer. The process creates the pedigree data record and sets up the association between the newly created data record and an unique item identifier such as the EPC number.

Extend: After the initialization or verification step, the pedigree is extended. The tracked data includes at least the item's unique identifier, the current (business) location, owner and a timestamp. The current owner signs the observation and contributes it to the shared pedigree record.

Share: After the owner extended the pedigree, the record must be made available to the next party that receives the physical item. This step is called "share pedigree". It involves the elaboration of the next destination and identity of the next owner. The process step is basically the transferal of access control of the pedigree from one party to the next.

Accept/Verify: After getting access control by proving the ownership, the new owner retrieves the electronic pedigree, identified by the EPC number. At this point, the current owner must be sure that the data contributed by the predecessors are correct. This process is called verification. After the successful verification, the new owner can continue the process and extend the pedigree.

5.2. Approach

We measure interaction costs by assessing the number of interactions needed to complete a process. By this approach, the results of different architectures

can easily be compared. The unit of analysis focuses on the processes of electronic pedigree that are "initialize", "extend", "share", "accept/verify". As the dynamic behavior of an electronic pedigree system should be assessed, this paper focuses on the latter three ones. For simplification, only the essential interactions are considered. The identification of essential interactions has been conducted on a "need-to-know" basis: what minimal input is required for a process step to achieve the desired outcome. Error handling or potential system failure is not taken into account. For calculating costs we use weighting factor 1 for each interaction. Figures 4-6 are used to depict the interaction scenes of the processes of different architectures. Only arrows from the initiator of an interaction are shown on the figures to keep them simple. Table 1 shows a short description of the interaction parameters that were used.

Table 1. Labels

Label	Description
Identity X	Identity of organization X
Credentials X	Digital identity of organization X and proof of identity
EPC	Unique identifier of physical object
Pedigree	Electronic pedigree associated with the physical object
Pedigree entry	Entry that is appended to the existing electronic pedigree

5.3. Compared architectures

The following figures indicate the flow of processes arranged over time. At organization A, the item has already passed the "accept/verify" step. For simplification, just one loop of the process is depicted. As the electronic pedigree is an information sharing application, the important architectures directly emerge from the models of information sharing presented in Section 2, namely information transfer, information hub and information hub combined with Dual Ownership.

5.3.1. Information transfer architecture

In the information transfer scenario (Figure 4), organization A is in possession of the complete pedigree. To extend the pedigree, only the EPC number of the item and the signed pedigree entry are necessary. After the extension, the pedigree may be shared with the next party. To prevent process hold up, the pedigree must be available at B before the arrival of the item. As the destination is known, A will send a request to its internal information system that identity B should be sent the pedigree of the item identified by the EPC number. In order to be reliable, B must also receive appropriate credentials from A in combination with the pedigree, to integrate the received pedigree into the information system of B. After the item arrived at B, B will use the EPC number to find the appropriate pedigree and verify the pedigree. Note that B will probably not only have to verify the signature of A framing the pedigree but also the individual signatures of the events. Otherwise, A could create a fake pedigree and introduce this one into the supply chain. Potentially, a system can be designed to work securely with only the verification of the last signature. In our model, we therefore refer to this as the "information transfer (optimized)" approach.

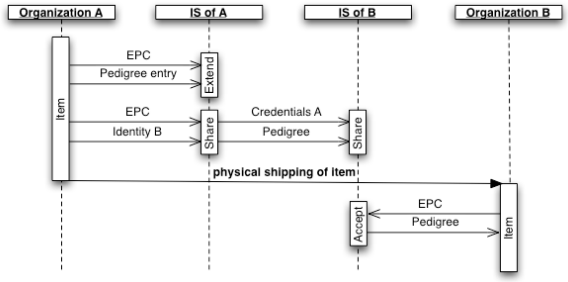

Figure 4. Information transfer

5.3.2. Information hub architecture

In the information hub architecture, a neutral party operates a central pedigree service (Figure 5). The complete pedigree is stored in a back-end database, which is not directly accessible by any party. Only operations offered by the service may be used to extend or retrieve the pedigree. The completeness and integrity is therefore ensured. For each operation, the service requires users to present their credentials to prove their identity. When organization A intends to add an entry to the pedigree of an object identified by its EPC number, it has to present the event data as well as appropriate user credentials. After the extension, organization A may want to share the pedigree with the intended recipient B of the item. Since A is the current owner of the object, A needs to instruct the service to transfer access rights to B. For this operation, A has to present its user credentials, the EPC number in concern and the recipient's identity. After the physical shipping to B, B confirms the arrival by presenting the user credentials and the EPC number to the pedigree service. The pedigree service returns the electronic pedigree and leaves B in control.

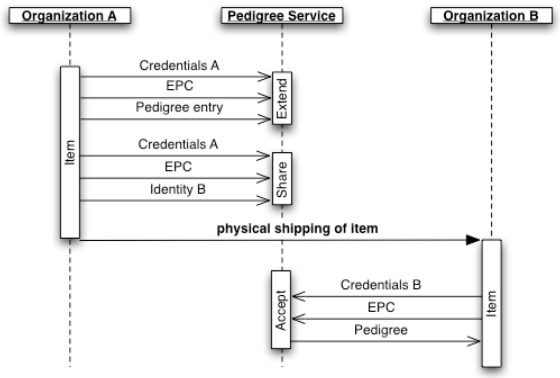

Figure 5. Information hub

5.3.3. Information hub combined with Dual Ownership

The information hub architecture combined with Dual Ownership also bases on a neutral pedigree service (Figure 6). But while the extend process step is identical to the one in the information hub model; the share process step is completely different. As access control is based on physical possession, the item is simply shipped to organization B.

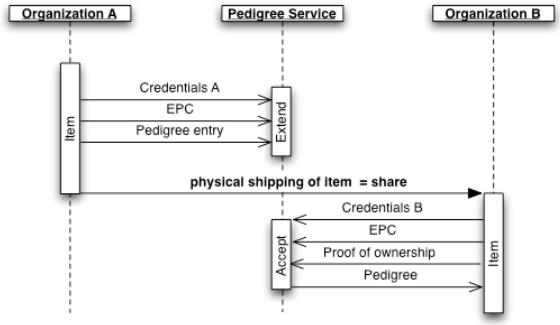

Figure 6. Information hub w. Dual Ownership

As the item arrives at organization B, B requests access rights by proving the ownership of the item. To prove the ownership and retrieve the pedigree, B sends its user credentials, the EPC number in concern, the proof of ownership (cf. Section 4.2) to the pedigree service.

5.4. Results

Based on the interaction flows depicted in the previous sections, interaction costs per step can be derived. Each interaction is weighted with the score 1. Additionally to the positive flow, the case of changing a shipping destination is investigated. Changes in destinations are highly relevant in today's dynamic supply chains. The "change destination" process step copes with the case of an unexpected or late change of the shipping destination. The interaction costs are reflecting the effort for executing the "share" process again.

Table 2. Interaction costs per step

	extend	share	accept/ verify	change dest.
Information transfer	2	4	n+1	4
Information transfer (optimized)	2	4	2	4
Information hub	3	3	3	3
Information hub with Dual Ownership	3	0	4	0

Table 2 shows the interaction costs per step. Note that in the information transfer architecture the "accept/verify" process depends on the number of partners (cf. Section 5.3.1). While the information transfer architectures need the fewest interactions in the "extend" process, the information hub models win in the "share" and the "change destination" processes. With only seven interactions for the standard process loop, the Dual Ownership model requires the least amount of interactions.

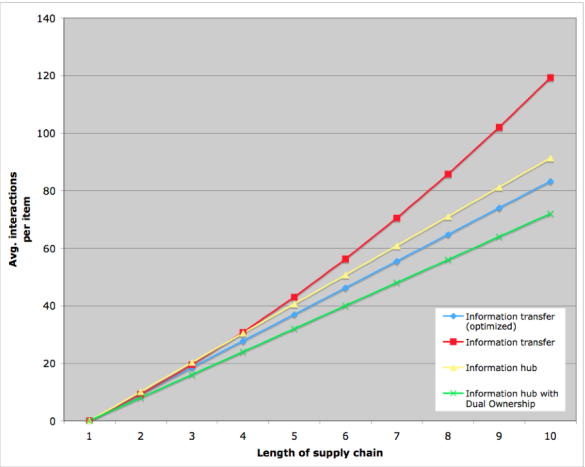

Figure 7. Varying length of supply chain

To visualize the dynamic complexity of the architectures, a typical sample scenario is selected. The sample scenario consists of a supply chain with varying length from one to ten. The length of ten is reasonable when looking at a supply chain consisting of tier 1-3 suppliers, the manufacturer, a distributor, a retailer and logistics service providers in between. It is

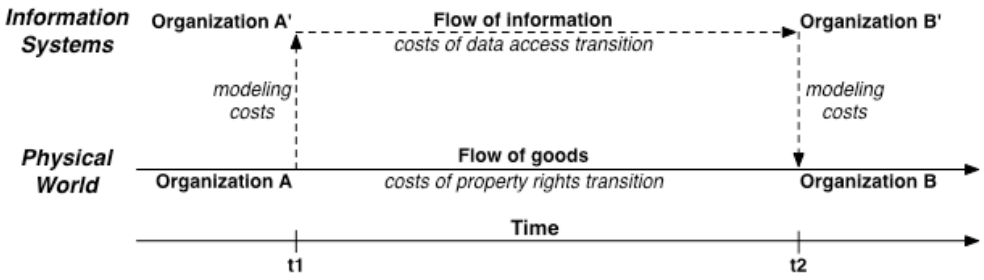

Figure 8. Cost saving due to Dual Ownership

assumed that a change of destination occurs at least with the probability of 1%. Figure 7 illustrates the results. Also in a dynamic context, Dual Ownership has the least complexity. Followed by the optimized information transfer model, the information hub model and the ordinary information transfer model. Even though the results of this evaluation are merely indicative, the potential of Dual Ownership is clearly visible. At a supply chain with the length of 10 partners, Dual Ownership needs 14% less interactions than the second best solution and over 40% less interactions than the information transfer solution.

6. Discussion

As illustrated in Section 5, Dual Ownership requires the least interactions already on a single item comparison with other solutions. The following part discusses where the information transfer and the information hub approach have always additional costs for modeling reality into information systems compared to Dual Ownership. We argue that this effect of cutting modeling costs can be even greater in more complex applications than electronic pedigree.

As depicted on Figure 8, each organization has besides its real identity A, a virtual identity A'. When shipping an item from A to organization B, the access to the electronic pedigree should be transferred as well. In order to transfer the access control, A has to find B', the virtual representation of B, in order to transfer the access. In the information transfer model, A has to prove the source identity A' to B'. In the information hub model, A' and B' need to prove their identity to the hub in order to start the data access transition. These costs for modeling the identities are depicted in Figure 8 as arrows between the physical world and the information systems. In addition, the transaction of the physical property right transition needs to be translated to information systems. The access permission needs to be transferred and then matched back to the electronic pedigree of the concerned item. Note that also the timing is crucial. If the item would arrive at organization B and the electronic pedigree is not accessible, this would cause a hold up in the process. For that reason, the process will be designed to transmit the access control to the destination before the physical product is shipped. A last-minute change of the physical shipping destination would in most cases need a rollback or repetition of the data access transition.

Decisions for late changes in shipping destinations often affect larger groups or even whole batches of items. In the evaluation of Section 5, the assumption of 1% probability for single item rerouting seems therefore too low. A higher rate of unexpected or late rerouting of items clearly emphasizes the advantages of Dual Ownership. In the Dual Ownership model interaction costs for information sharing associated with unexpected rerouting of items equal zero, while the costs in other approaches would increase significantly.

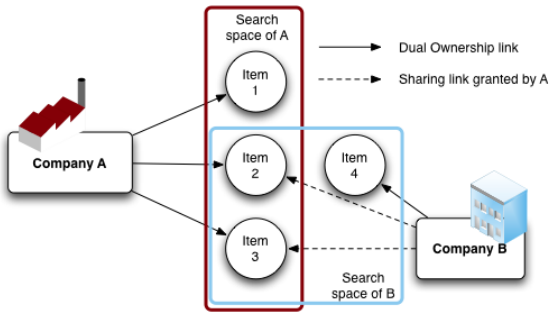

Figure 9. Segmented search spaces

For real world implementations, it is not only important to understand in which scenarios Dual Ownership can provide cost advantages, but also what Dual Ownership means for a large-scale application. While this paper mainly illustrated the concept by means of single item examples, a real world scenario would need operations to handle multiple information assets at once. The key feature to access multiple assets is a search module. A service that implements the Dual Ownership model must ensure that its search and retrieval interfaces follow the same principles. For example, in a service that allows owners to grant

access to remote parties for certain information assets, the search space of party A and B (Figure 9) must be segmented. The number of items in a search space is highly dependant on the ownership and granted access to assets. Normally, a search service indexes all available records and provides a query interface to retrieve specific results. Following the Dual Ownership model, the search space must be restricted according to the identity of the enquirer. As a consequence, only users with established Dual Ownership links can execute queries and retrieve most recent data records. Otherwise, previous owners would be able to retrieve future data beyond their item possession without consent of the current owner.

7. Conclusions and future work

To fight increasing safety threats due to counterfeits, regulation bodies force pharmaceutical supply chains to electronically document the chain of custody of individual items. This inter-organizational application relies on information downstream sharing and thus the transferal of access control from one organization to the next. To connect existing access control models within organizations on an inter-organizational stage, a novel model, called Dual Ownership was presented. Instead of continuously remodeling access control into information systems, Dual Ownership utilizes the property of physical possession as proof for transferred access control. The result would be additional security by providing communication encryption and privacy protection. To outline the advantages of electronic pedigree combined with Dual Ownership, three architectures have been evaluated and compared. The results indicate that Dual Ownership offers clear advantages by reducing modeling costs for access control transferal. The discussed effect for reduced modeling costs may be even greater in other applications. Therefore, future work will try to explain and generalize the effect of Dual Ownership. Field trials with different application scenarios and industries will be conducted to ground the findings. Another future research field is the development of new database models optimized for item-level information sharing. Databases need to provide efficient search and store operations to cope with high data volumes and user-specific search spaces that can change very quickly.

Acknowledgements

This work was partly funded by the European Commission within the Sixth Framework Programme (2002-2006) IP Nr. IST-FP6-033546.

8. References

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

[2] World Health Organization, "Fact sheet No. 275," 2006; http://www.who.int/mediacentre/factsheets/fs275/en/index.html

[3] U.S. FDA, "Curbing Counterfeit Drugs," 2006; http://www.fda.gov/fdac/features/2006/506_counterfeit.html

[4] D, Molnar, A, Soppera, and W. D., "A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags," Workshop in Selected Areas in Cryptography, 2005

[5] 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.

[6] H.L, Lee, and W. S., "Information sharing in a supply chain," International Journal of Technology Management, 20(3), 2000, Inderscience, pp. 373–387.

[7] M. Harrison, and T. Inaba, "Improving the safety and security of the pharmaceutical supply chain," 2006; http://www.autoidlabs.org/uploads/media/AUTOIDLABS-WP-BIZAPP-030.pdf

[8] U. Hengartner, and P. Steenkiste, "Exploiting information relationships for access control in pervasive computing," Pervasive and Mobile Computing, 2(3), 2006, pp. 344-367.

[9] I, Foster, C, Kesselman, and T. S., "The Anatomy of the Grid: Enabling Scalable Virtual Organizations," International Journal of High Performance Computing Applications, 15(3), 2001, pp. 200–222.

[10] A. Juels, "RFID security and privacy: a research survey," IEEE Journal on Selected Areas in Communications, 24(2), 2006, pp. 381-394.

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

[12] 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.

[13] 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.