Expressive RFID data access policies for the Pharmaceuticals supply chain

Miguel L. Pardal[†], Mark Harrison[‡], Sanjay Sarma[§] José Alves Marques[†]

[†]Department of Computer Science and Engineering
Instituto Superior Técnico, Technical University of Lisbon, Portugal
Email: miguel.pardal@ist.utl.pt, jose.marques@link.pt

[‡]Auto-ID Labs, Institute for Manufacturing, University of Cambridge, UK
Email: mark.harrison@cantab.net

[§]Auto ID Labs, Massachusetts Institute of Technology, USA
Email: sesarma@mit.edu

***Abstract*—The Pharma(ceuticals) industry is at a cross-roads. There are growing concerns that illegitimate products are penetrating the supply chain. There are proposals in many countries to apply RFID and other traceability technologies to solve this problem. However there are several trade-offs and one of the most crucial is between data visibility and confidentiality.**

In this paper, we use the *TrakChain* assessment framework tools to study the US Pharma supply chain and to compare candidate solutions to achieve traceability data security: Point-of-Dispense Authentication, Network-based electronic Pedigree, and Document-based electronic Pedigree. We also propose extensions to a supply chain authorization language that is able to capture expressive data sharing conditions considered necessary by the industry's trading partners.

I. Introduction

Radio-Frequency Identification (RFID) [1] enables higher resolution traceability information systems. Physical objects can be tagged with transponders and then can be detected automatically by interrogators placed at strategic business locations. With RFID, traceability events – *when* and *where* the object was observed – can be captured more often and more accurately than with other technologies.

Traceability information systems enable the retrieval of past (*trace*), present (*track*) and possible future information (*predict*) [2]. *Tracing* finds the historical states of a physical object. *Tracking* refers to finding the current state of an object, such as its current location. *Prediction* provides a probabilistic view of future states.

Trace is a complete supply chain pedigree (history) of a given product. It is an *upstream* view of the supply chain from the perspective of the current owner.

Track is to simply know where the product is. It is a *downstream* view, usually from the perspective of the manufacturer.

This kind of capability is relevant to many industries [3]. In particular, the Pharmaceuticals industry is at a turning point. There have been documented cases [4] of illegitimate drugs reentering the legitimate supply chain. This endangers patients and reduces the public's trust in brand names.

Around the world, there is a shared understanding of the challenges facing Pharma supply chains. Nevertheless there are different views of the solution. In the European Union (EU) [5] and other countries the proposed solution is *Point-of-Dispense Authentication (PoD)* that verifies the authenticity of products on both ends of the supply chain: manufacturers and pharmacies. In the United States of America (US) the proposed solution – already law in some states – is typically *electronic Pedigree (eP)* that records the chain-of-ownership of the products.

Both PoD and eP require that the products be identified with unique serial numbers. The current proposals state that item-level identifiers are encoded using printed two-dimensional bar-codes – GS1 DataMatrix [6] – and container-level identifiers are stored in RFID tags. However, the GS1 identifier architecture[1]provides a data carrier compatibility layer [7] that will allow a gradual transition from bar-codes to RFID tags.

Marking products with unique identifiers is necessary but not sufficient to achieve visibility in the supply chain. The trading partners need to be willing to share the data but no one wants to share information with commercial value unless there is a security policy and a trust domain [8]. Companies need to trust that their data will be used only for the intended purpose and that it will not be abused e.g. by competitors to learn about business strategies and initiatives in advance.

The work presented in this paper focuses on an assessment of traceability information systems for the US supply chain, comparing Point-of-Dispense Authentication, *Document-based* and *Network-centric* electronic Pedigree solutions. The goal is strengthening the security of the supply chain through enhanced visibility control.

The US Pharma supply chain was selected because it is well documented, with recent statistics collected in the latest edition

[1] **G**lobal **S**tandards **1** is the organization that oversees the most widely used supply chain standards system.

of the HDMA[2] Fact Book [9]. For estimating the cost of the overall architecture we will use the *TrakChain* assessment framework traceability cost model [10].

Extensions are proposed to the Chain-of-Trust Assertions (CTA) implementation of SCAz (Supply Chain Authorizations) [11] that uses the Resource Description Framework (RDF) and other Semantic Web technologies [12].

A summary characterization of the *US Pharma supply chain* is presented next. A qualitative assessment of the threats and proposed protections for supply chain safety is also presented. The extensions to the supply chain authorization language, SCAz, are proposed and discussed in Section III. The TrakChain assessment framework is introduced in Section IV and its tools are used to characterize the considered traceability systems and finally an evaluation of the proposed system is presented in Section IV-A. The paper concludes with key contributions and future work opportunities.

II. US Pharmaceutical Supply Chain

The great majority of drugs dispensed in US pharmacies [9] are initially sold by a manufacturer to a distributor, who then sells them to the dispensing pharmacy[3]. The Pharma supply chain has around 1,400 manufacturers, 70 distributors, and 166,000 pharmacies. More than 90% of the volume of drugs passing through the supply chain goes through only three distributors. The vast majority of drugs sold in the U.S. pass through only a single wholesaler on its way from the manufacturer to the pharmacy, making the *average chain length* equal to 3.

The average distribution center handles about 50,000 stock keeping units (SKU), where each code is used to identify each unique product classes or items for sale.

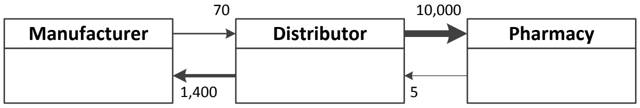

Fig. 1. US Pharma supply chain associations with typical cardinalities.

Figure 1 represents the "connections" between trading partners that represent both business relationships and network connections [13]. The typical *manufacturer* wants to maximize the availability of its products, so it works with as many distributors as it can handle (up to 70 connections). The typical *distributor* (wholesaler) sources from most manufacturers (1,400) and sells to a large number of pharmacies, whether as a primary source or as a secondary source. The three largest distributors each sell and deliver to about 10,000 pharmacies. The *pharmacy* buys their drugs from a primary distributor and, if that distributor is out-of-stock, from secondary sources (up to 5 sources).

A. Electronic Data Interchange

The HDMA has published EDI (Electronic Data Interchange) guidelines that are followed by trading partners to exchange structured business data in electronic form. The guidelines are based on the ASC X12 variant of EDI, the most used in North America. The following transactions (messages) are relevant for this work because they transmit item identifiers that can be extracted and used to define data sharing policies:

- 810 – Invoice;
- 850 – Purchase Order (PO);
- 855 – Purchase Order Acknowledgement;
- 856 – Advance Ship Notice (ASN).

For example, an 856 ASN document informs a trading partner about a shipment of goods arriving at a location.

B. Threats

Unfortunately, the HDMA report [9] confirms that counterfeit drug cases are on the rise.

Past problems [4] have led larger wholesalers to make a pledge to increase the security of the supply chain: **only buy drug supplies directly from the manufacturers**. Nevertheless, there are possible attacks:

1) Wholesalers ignoring their pledge.
2) (Small) wholesalers who are unable to make the pledge to only buy directly from the manufacturer.
3) Returns of counterfeit or stolen products in replacement of legitimate products through a wholesaler.
4) Criminal wholesalers or pharmacists/pharmacies.

Security mechanisms are designed to prevent illegitimate products from entering the supply chain through these vulnerabilities. The next section discusses the protections being proposed to increase the security of the supply chain: PoD and two eP alternatives.

C. Protections

In a PoD (Point-of-Dispense) security model, only the two ends in the Pharma supply chain need to collaborate: the manufacturers and the pharmacies. The PoD system keeps track of unique serial numbers commissioned by manufacturers and consumed at the point of dispensing to a patient. In between, checks are also possible but optional.

In a eP (electronic Pedigree) security model, the chain-of-ownership is tracked and its legitimacy is checked by each new owner as the drug moves down the supply chain. There are document-based and network-centric approaches to eP.

DPMS (Drug Pedigree Messaging Standard) [14] is a GS1 standard for *Document-based eP* (DeP) that was specifically created to assist the Pharma supply chain with creating an interoperable system to trace drugs in a way that complies with existing drug pedigree laws. DPMS documents are self-contained and show the chain-of-ownership of a given product. Security is achieved with digital signatures [15].

EPC IS (Electronic Product Code Information Services) [16] is a GS1 standard that defines interfaces for capturing and querying traceability event data. A special event set can

[2] The **H**ealthcare **D**istribution **M**anagement **A**ssociation is an organization representing primary healthcare distributors in the U.S.

[3] Chain pharmacies have their own internal distribution networks and often buy high volume products directly from the manufacturers.

be defined for *network-centric eP* (NeP). These events are captured and stored in repositories and then used later for pedigree validation. The current NeP proposals state that the number of repositories should be limited and well-known, entailing a semi-centralized architecture.

III. Pharma Supply Chain Authorizations

The data visibility and confidentiality requirements are described next, derived from an industry NeP pilot currently in progress. New authorization assertions are proposed to comply with the requirements of the Pharma supply chain.

A. Visibility and Confidentiality

The supply chain visibility model in current use throughout the US Pharma supply chain is the "one up-one down" model. Each trading partner knows who they bought the products from ("one up") and who they sold the products to ("one down"). Each trading partner does not know where the drugs came from prior to their immediate supplier.

This model protects business confidentiality but is insufficient to protect consumers from illegitimate products. Data about an individual physical object should be shared by the companies in its chain-of-custody, at least. More protection requires upstream traceability data that must be explicitly authorized to be accessed. However, in most supply chain situations the information owner does not have sufficient prior knowledge about the partners who should be authorized to view the information, because the path taken by each object only emerges over time, rather than being fully pre-determined at the time of commission.

1) Pilot: The NeP pilot project has been implemented by a service provider (GHX) involving a manufacturer (Abbott Laboratories), a distributor (McKesson) and a dispenser (Veterans Administration hospital) [17]. Several surveys were conducted for this pilot to establish the functionalities and default visibility policies required by the participating companies [18].

Regarding visibility policies, the *pharmacy* sees all the chain-of-custody events only for the product they receive, from the manufacturer through any intermediaries in the supply chain. The *distributor* can see all the history prior to acquisition of the drug and its own events. It can see the pharmacy's receive event. From that point on, the information is filtered. The *manufacturer* can see its own events and the receiving event of the distributor, but after that all the information is carefully filtered to remove the company location identifiers and none of the downstream consistency checks are shown. The *service provider* would hold all of the data but the ownership rights – and policy authoring rights – would remain with the trading partner who generated each event. Every member of the supply chain owns the events that they contribute. The service provider would provide the service of automated sharing of that data, as controlled by the data owner's policies.

There is a need to express delegated and transitive trust because it is likely that the manufacturer does not know the final destination of the products. Also, a partner may require additional conditions for sharing data. And there must be ways to define trust for sets of products and sets of partners, otherwise the administrative burden of authorizing individual items can quickly become overwhelming.

B. Implementation

Supply Chain Authorizations (SCAz) allows authorizations for accessing traceability data to be expressed with concepts such as item, company, etc. SCAz has several implementations for the same API, but the one with the most expressive potential and with average performance is Chain-of-Trust Assertions (CTA) [11], implemented using the Apache Jena Semantic Web tool kit.

CTA expresses access rights as logical statements, called *assertions*, that are issued by participants in the supply chain.

1) Explicit trust: CTA requires explicit trust assertions to grant read access to traceability records. Figures 2 and 3 show a textual and visual representation of a simple CTA policy expressed as subject-predicate-object RDF triples [19].

```
:company0  a  cta:Organization .
:company1  a  cta:Organization .

:item0     a  cta:Identifier .
:record0   a  cta:Record .
:policy0   a  cta:Policy .

:company0  cta:publishes   :record0 .
:record0   cta:about       :item0 .

:company0  cta:creates     :policy0 .
:policy0   cta:protects    :item0 .
:policy0   cta:grantsRead  :company0 .
:policy0   cta:grantsRead  :company1 .
```

Fig. 2. CTA Policy in RDF Turtle format, including type definition predicates (rdf:type abbreviated as 'a').

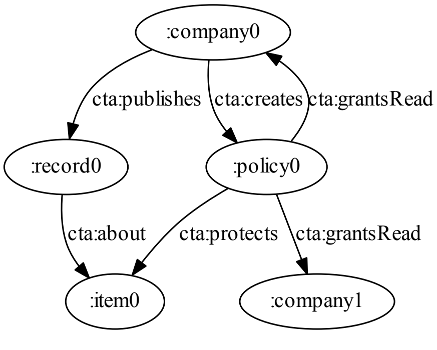

Fig. 3. CTA Policy graph.

In the example, 'policy0' created by 'company0' (the data owner) grants read access to 'record0' about 'item0' to itself and to 'company1'. The policy can be extended with new assertions e.g. 'cta:grantsWrite'.

Identifier data can be extracted from EDI transaction documents exchanged between the business partners, such as the ones mentioned in Section II-A.

The policy can be converted to the XACML (eXtensible Access Control Markup Language) [20] standard authorization policy language. The conversion procedures are based on previous work by Karjoth et al. [21] and are described in [11].

2) Delegated Trust: The first extension to CTA is to add support for the *delegation* of administrative rights from one organization to another, as represented in Figure 4.

company0 delegates the ability to grant access to company1, and company1 grants read access to company2. company0 does not have to know company2. Access is granted if there is an explicit unbroken chain of trust assertions leading back to the owner of the data.

```
:company0  cta:publishes   :record0 .
:record0   cta:about       :item0 .

:company0  cta:creates     :policy0 .
:policy0   cta:protects    :item0 .
:policy0   cta:delegates   :company1 .
:policy0   cta:grantsRead  :company2 .
```

Fig. 4. CTA delegation extension (type definition predicates omitted).

RDF has a query language called SPARQL [22] that simplifies navigation of the graphs. SPARQL can also be used to construct new RDF triples using specified inference criteria. To verify the delegated trust, two *construct* statements are used. The first statement is used to compute the delegation path. It checks if the 'cta:delegates' predicates chain forward. The second statement verifies if the read access is granted by anyone in the trust chain.

3) Transitive trust: Trust for data regarding a specific item sometimes needs to be *transitive*. The predicates represented in Figure 5 are designed to express *dynamic* chain upstream/-downstream conditions, allowing data sharing between parties that did not have previous interactions. By issuing the 'cta:trustChain' predicate, 'company0' allows 'company1' to access 'record0' about 'item0' because it published 'record1' about the same item.

```
:company0  cta:publishes   :record0 .
:record0   cta:about       :item0 .

:company0  cta:creates     :policy0 .
:policy0   cta:protects    :item0 .
:policy0   cta:trustChain  :item0.

:company1  cta:publishes   :record1 .
:record1   cta:about       :item0 .
```

Fig. 5. CTA chain trust transitivity extension (type definitions omitted).

4) Conditional Trust: Trading partners can issue *conditional* assertions, like reciprocal trust: "I trust you if you trust me". The reciprocal trust predicates are represented in Figure 6. The 'cta:grantsReadRecipr' issued by 'company0' is only effective if a similar predicate is issued granting conditional access to records about the same item.

```
:company0  cta:publishes         :record0 .
:record0   cta:about             :item0 .

:company0  cta:creates           :policy0 .
:policy0   cta:protects          :item0 .
:policy0   cta:grantsReadRecipr  :company1.

:company1  cta:creates           :policy1 .
:policy1   cta:protects          :item0 .
:policy1   cta:grantsReadRecipr  :company0.
```

Fig. 6. CTA reciprocal trust extension (type definitions omitted).

5) Bulk trust: So far the data sharing policies have addressed individual items and individual companies. However, considerable efficiencies can be obtained by representing object groupings (lots) and company sets (groups).

There are three ways of modelling relationships with cardinality greater than one in RDF. The first, and simplest, is to define multiple values for a predicate. The second uses 'head' and 'rest' predicates to create a linked list and is intended for closed, ordered collections. The third uses types and special ordinal predicates to define the items that belong to the collection. There are ordered (*Sequence*) and unordered (*Bag*) collections.

Figures 7 and 8 represent a trading partner group and a lot: lot0 contains 3 items; group0 contains 2 companies. For the product set – lot – multiple predicate values were used because it is a simpler, less verbose approach that is suitable for relationships without attributes. The lot object can be further characterized, with predicates for it. For the trading partner group a 'Bag' was used because it provides an identity to the collection and allows further characterization of the relationship. Also the cardinality of the relationship is expected to be much smaller than the lots that will easily reach thousands of items.

```
:group0 cta:group [
    a       rdf:Bag;
    rdf:_1  :company0;
    rdf:_2  :company1
].

:lot0   cta:inLot  :item0.
:lot0   cta:inLot  :item1.
:lot0   cta:inLot  :item2.
```

Fig. 7. CTA bulk trust.

IV. TrakChain

The PoD, NeP and DeP security proposals for the US Pharma supply chain were assessed using the TrakChain cost model .

TrakChain is a traceability information system assessment framework. The motivation to build it came from the fact that the development and deployment of traceability applications implies significant up-front costs: tags, readers, and their installation at all relevant business locations. The integration with existing information systems is also challenging [23].

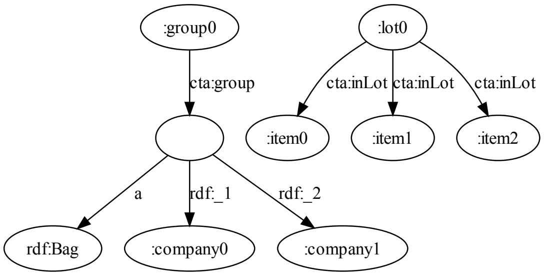

Fig. 8. CTA bulk trust graph.

Many times it is unclear what is the best system architecture for a given supply chain problem, so it is useful to estimate the cost of traceability information systems, and have a preview of the size and cost of the system.

TrakChain includes the following tools:

- Traceability cost model [10] – analytical model of systems that allows a cost-effective evaluation when there is no access to implementations of the target system; it is based on previous work by Murthy and Robson [24];
- Cost calculator – extension of the cost model with a cause-effect cost calculation black-board [25] that allows the separate consideration of different concerns for more detailed calculations e.g. security mechanisms' overheads;
- SCAz – supply chain authorization policies implementation and tool to verify correctness and measure performance of prototype instances.

The first tool is used for the PoD, NeP, and DeP cost assessment. The third tool was used to develop the supply chain security policies of Section III.

The framework's use is depicted in Figure 9. The information system is specified in three aspects: the *functional scheme* of the components outlines what are the parts of the system and their interactions; the *partition scheme* specified how data is distributed by instances of the system; the *security scheme* details the security infrastructure. When the schemes are combined, a system is modelled to compute cost estimates or can be implemented and instrumented to produce measurements. The estimates can then be compared to measurements, allowing the model to be validated and calibrated.

A. Assessment

The first step in our assessment of traceability systems is to classify it according to two criteria: data integration and centralization. PoD, NeP and DeP solutions are classified in Figure 10. Data integration specifies if the system copies data (*copy*) or refers to it (*refer*). Centralization specifies if the system has special nodes (*centralized*) or not (*decentralized*). In the particular case of the Pharma chain the 'refer' possibility is not used because the industry considers an unacceptable risk to build a system that fulfils a legal requirement depending on the availability of trading partners' data.

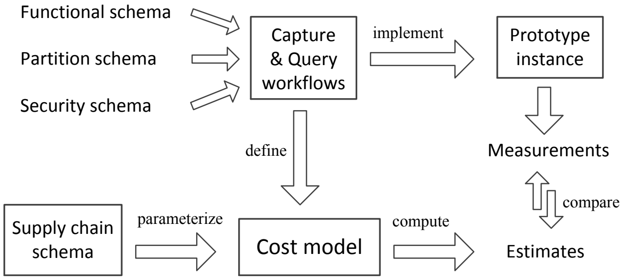

Fig. 9. TrakChain assessment framework.

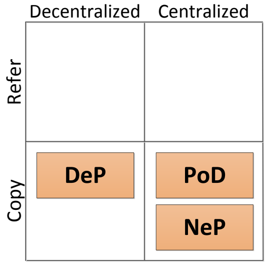

Fig. 10. Pharma traceability system classification.

PoD is centralized and copies identifier usage data to a special repository node. NeP is also centralized but copies more data – EPC IS events – to the pedigree repository. DeP is decentralized because the DPMS pedigree records are not stored in any special node, and the accumulated data is copied along the supply chain.

Each of these solutions was modelled using the cost model.

1) Point-of-Dispense Authentication: Figure 11 represents a PoD solution, including the cardinalities of the data exchange connections. The PoD repository keeps product instance data. A Public-Key Infrastructure (PKI) [26] is represented because cryptographically strong authentication is required before product identifier data is published (by a manufacturer) or queried (by a pharmacy).

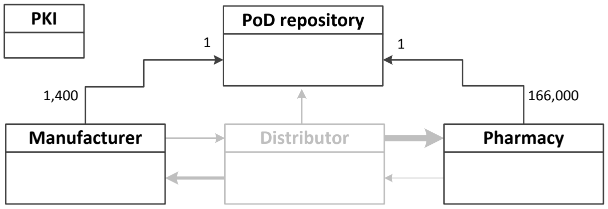

Fig. 11. PoD data exchange connection cardinalities.

As represented in Figure 11, on commission of a new product (id), the manufacturer sends a message to the PoD repository to register new identifiers.

On sale of a product, the pharmacy sends a message to the PoD repository to verify that the identifier is still unsold.

There can be additional identity checks, usually triggered by a random test or by a specific suspicion. On suspicion, the trading partner (e.g. a wholesaler) checks if the identifiers belong to the expected manufacturer and are fit for sale.

2) Network-based electronic Pedigree: Figure 12 represents a NeP solution, including the cardinalities of the data exchange connections. We assume a semi-centralized model, where each trading partner connects with a small number of service providers (just 1 in the Figure). The NeP repository implements the EPC IS interfaces, extended with a pedigree checking service.

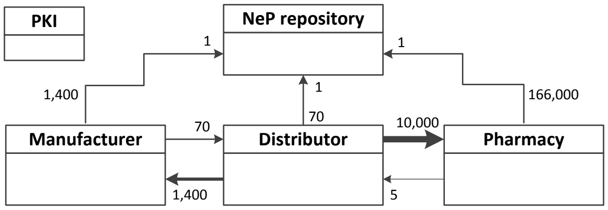

Fig. 12. NeP data exchange connection cardinalities.

For outgoing products, an EPC IS event must be published (e.g. with business step 'shipping').

For incoming products[4], a query is issued to the checking service, that will apply the relevant pedigree regulations. When the physical products actually arrive, and EPC IS event is published with bizstep 'receiving'.

Aggregate add/delete events required to keep track of container transports are being omitted for simplification.

3) Document-based electronic Pedigree: Figure 13 represents a DeP solution, including the cardinalities of the data exchange connections. There is no centralized support service in this case.

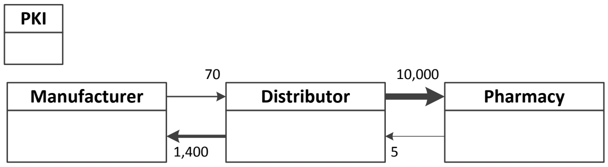

Fig. 13. DeP data exchange connection cardinalities.

For outgoing products, a new record is appended to the pedigree, and a new digital signature is added.

For incoming products, the public key certificates must be retrieved from the PKI to verify the pedigree.

B. Secure connections

Secure data exchange connections are required for all solutions; in PoD and NeP to connect to the centralized services; in NeP to connect the trading partners in the object's path.

The trust required for the digital signatures means that each trading partner needs an account in a PKI.

The cost of set-up involves the creation of a key pair, and the emission and sharing of public key certificates. This procedure can be added to the existing accreditation procedures already practised by most companies [9].

Table I shows the assessment of the required secure connections upstream, downstream and other, for the PoD solution. NeP is the same in this regard. Table II assesses the DeP case. The sub-total is the number of connections for a single instance. The total is the number of connections for the whole US Pharma Supply Chain (refer to the cardinalities of Figures 11, 12, and 13 for the multiplier values).

	up	down	other	sub-total	total
Manufacturer	0	0	1	1	1,400
Distributor	0	0	1	1	70
Pharmacy	0	0	1	1	166,000
					167,470

TABLE I
PoD AND NeP REQUIRED SECURE CONNECTIONS.

	up	down	other	sub-total	total
Manufacturer	0	70	0	70	98,000
Distributor	1,400	10,000	0	11,400	798,000
Pharmacy	5	0	0	5	830,000
					1,726,000

TABLE II
DeP REQUIRED SECURE CONNECTIONS.

Clearly the centralized approaches – PoD and NeP – require less set-up effort for most trading partners, because less key exchanges need to be done. Choosing DeP represents a *tenfold* increase in the number of required secure connections.

C. Estimates

The cost model's parameters are presented in Table III and capture characteristics of the system, application, and chain.

Type	Name	Symbol	Unit	Value
System	Bandwidth	β beta	bps	10^9
System	Processing speed	γ gamma	bps	10^9
System	Seek time	θ theta	ms	1
App.	Message size	μ mu	bit	10^5
App.	Item record size	δ delta	bit	10^5
Chain	Avg. length	z	vertex	3

TABLE III
COMMON PARAMETERS.

According to the HDMA Fact Book [9], a typical Pharmaceuticals Distribution Center handles an average of 100,000 items per day. The cost model produced estimates assuming this number of items as the central value in the following plots.

Figure 14 represents the storage costs. The data volumes of tens of gigabytes per working day for the distribution center are within the reach of available technology. The DeP solution has the greatest overall storage requirements, significantly greater than NeP and PoD, because the partial pedigree records are kept at each trading partner. PoD stores less information than NeP because it only has to keep track of identifier usage whereas NeP records more detailed events.

[4] The pedigree check can be triggered as soon as a 856 ASN is received.

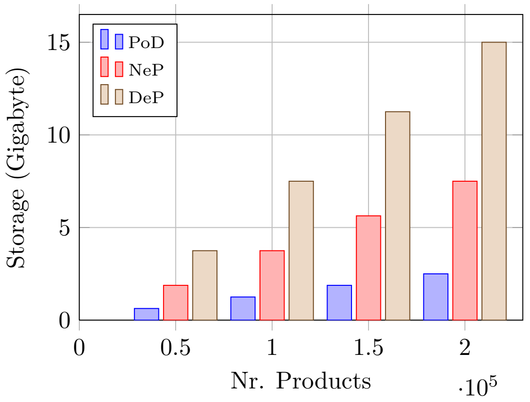

Fig. 14. Total storage cost for capture.

Figures 15 and 16 represent the time costs of the data capture and query operations, respectively. The time cost considers both time spent on processing and time spent on network communications.

The considered time values spent (hundreds of seconds) are small for a working day with 8 hours (28,800 seconds).

The cost of the capture is smaller for the PoD, because only two operations are needed, at both ends of the supply chain. The cost for PoD is independent of the chain length.

NeP spends time communicating with the central repository. DeP spends (a little less) time communicating with the next trading partner in the chain. In both cases, the cost is dependent on the length of the supply chain ($z = 3$).

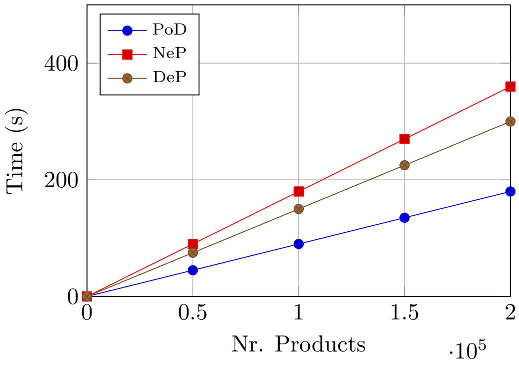

Fig. 15. Total time cost for capture.

The cost of query is smaller for DeP, because only local records have to be retrieved. The cost of the PoD is next because it only queries the identifier state. NeP has more cost because it retrieves the complete pedigree record from the repository. Alternatively, it could also just return a state. In that case, the cost would be similar to PoD.

V. Conclusions

This paper presented specific business solutions made possible by the capabilities of RFID technology and other data carriers of serialized product identifiers.

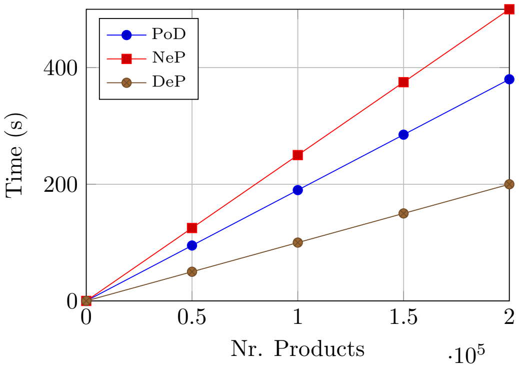

Fig. 16. Total time cost for query.

The assessment of the solutions started with a characterization of the US Pharma supply chain. In particular, the visibility and confidentiality was discussed and several extensions to a supply chain authorizations language were proposed and qualitatively evaluated. The default data visibility and confidentiality policies for the supply chain were based on findings from an industry survey for a pilot system. Additional conditions, such as those defined within trading partner contractual agreements, can be combined with default definitions to achieve *precisely* what the participants mean to share. Using the proposed extensions – delegation, chain trust, reciprocal and bulk – to the authorization language, the conditions required by the pilot requirements can be represented and used for flexible policy validation.

The overall conclusion is that it is possible to define expressive policies acceptable to industry trading partners that will also (re)use data from EDI documents.

Following the authorizations discussion, the proposed traceability systems were assessed using the TrakChain assessment framework. Having an actual business context further validated assumptions regarding query types and frequencies.

Estimates confirmed that PoD is the most lightweight approach and stores less information. It also requires a limited number of secure data exchange connections. This approach is lightweight but does not aid in criminal investigations, because the chain-of-ownership is not retained.

DeP stores the most data – partial pedigrees – across the chain, and also requires 10 times more secure connections. It is the most expensive solution. However, despite being the heaviest approach it does provide documentation that can be useful for criminal investigations and prosecutions when needed.

NeP is a middle ground between PoD and DeP. It stores more data than PoD, but assuming a semi-centralized architecture, it minimizes the number of secure data exchange connections.

An advantage of NeP is that separating the pedigree checking in a service is to allow the same infrastructure – EPC IS and the EPC network – to be used with different legal pedigree laws & regulations, and also for other traceability purposes, including recalls and providing more accurate data for other information systems. The security system can start with a PoD approach and then evolve to a full pedigree, reusing the existing parts of the system.

A. Future Work

The RDF assertion-based authorization performance will be measured with realistic workloads, given the load of a typical distribution center – the highest volume point in the chain – and the load of a pharmacy – the lowest volume point.

The RDF approach can be compared with Complex Event Processing (CEP) [27] technology that is especially designed for matching patterns in streams of events. Presumably, the performance can be increased by using it.

The extended policies defined in RDF can be converted to XACML, if necessary. This will allow policy interpretation portability in a standard authorization infrastructure, part of an externalized security architecture that is suited to cloud computing deployments [28]. Also, using a policy language standard makes sense for SCM (Supply Chain Management) applications because they involve multiple organizations.

RDF policies can also be integrated in widely used ERP (Enterprise Resources Planning) solutions, providing compatibility with existing authorization mechanisms, like the *SAP Authorization Concept* with users, roles, and actions [29].

RDF policies in the Pharma supply chain will probably be enforced in semi-centralized services. However, the proposed security framework can be used for distributed traceability systems, such as Object Naming Service and Discovery Services. These extended use cases will be implemented in the future.

Considering the whole system, if the traceability data authorization mechanism is trusted by trading partners then more data can be shared. Bar-codes can also contain lot number and expiry date. Using the GS1 identifier RFID and bar-code compatibility, high-value products can be identified by RFID tags and lower-cost products with bar-codes. RFID opens more possibilities for products with special transportation needs e.g. a product can be protected with RFID tags with built-in temperature sensor [30]. All of this additional data can be used to improve the US Pharma supply chain and keep more people safe from harm.

Acknowledgment

The authors acknowledge Dirk Rodgers for his insightful comments, and the HDMA for providing the EDI guidelines and other reference materials.

Miguel L. Pardal is supported by a PhD fellowship from the Portuguese Foundation for Science and Technology FCT (SFRH/BD/45289/2008).

References

[1] K. Finkenzeller and D. Muller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*. Wiley, 2010.

[2] Y. Wu, D. Ranasinghe, Q. Z. Sheng, S. Zeadally, and J. Yu, "RFID Enabled Traceability Networks: A Survey," *Distributed and Parallel Databases (Springer)*, 2011.

[3] E. W. Schuster, S. J. Allen, and D. L. Brock, *Global RFID: The value of the EPCglobal network for supply chain management*. Springer, 2007.

[4] K. Eban, *Dangerous Doses: How Counterfeiters Are Contaminating America's Drug Supply*. Houghton Mifflin Harcourt, 2005.

[5] EFPIA, GIRP, and PGEU, "European Stakeholder Model (ESM) - ensuring patients have access to safe medicines," June 2012.

[6] GS1, "The Value and Benefits of the GS1 System of Standards," GS1, Tech. Rep., 2010. [Online]. Available: http://www.gs1.org/docs/GS1_System_of_Standards.pdf

[7] ——, "RFID Bar Code Interoperability," GS1, Tech. Rep., August 2012, gS1 guideline. [Online]. Available: http://www.gs1.org/docs/gsmp/RFID_Barcode_Interoperability_Guidelines.pdf

[8] M. Eurich, N. Oertel, and R. Boutellier, "The impact of perceived privacy risks on organizations' willingness to share item-level event data across the supply chain," *Journal of Electronic Commerce Research*, vol. 10, no. 3-4, pp. 423–440, December 2010.

[9] HDMA, *HDMA Fact Book*. Healthcare Distribution Management Association, 2012-2013.

[10] M. L. Pardal and J. A. Marques, "Cost Model for RFID-based Traceability Information Systems," in *IEEE Int'l Conf. on RFID Technology and Applications*, September 2011.

[11] M. L. Pardal, M. Harrison, S. Sarma, and J. A. Marques, "Performance Assessment of XACML Authorizations for Supply Chain Traceability Web Services," in *8th Int'l Conf. on Next Generation Web Services Practices (NWeSP)*, November 2012.

[12] D. Allemang and J. Hendler, *Semantic Web for the Working Ontologist, Second Edition: Effective Modeling in RDFS and OWL*, 2nd ed. Morgan Kaufmann, June 2011.

[13] D. Rodgers, "U.S. Pharma Supply Chain Complexity," *RxTrace*, May 2011. [Online]. Available: http://www.rxtrace.com/2011/05/u-s-pharma-supply-chain-complexity/

[14] EPCglobal, *Pedigree 1.0*, GS1 Std., January 2007. [Online]. Available: http://www.epcglobalinc.org/standards/pedigree

[15] J. Biskup, *Security in Computing Systems - Challenges, Approaches and Solutions*. Springer, 2009.

[16] EPCglobal, *EPC Information Services (EPCIS) 1.0.1 Specification*, GS1 Std., September 2007.

[17] D. Rodgers, "The Significance of the Abbott, McKesson and VA Pilot," *RxTrace*, November 2012. [Online]. Available: http://www.rxtrace.com/2012/11/the-significance-of-the-abbott-mckesson-and-va-pilot/

[18] N. Basta, "Healthcare Exchange Bids for Prototyping a Track-and-Trace System," *Pharmaceutical Commerce*, April 2011.

[19] F. Manola and E. Miller, *RDF Primer*, W3C Std. [Online]. Available: http://www.w3.org/TR/2004/REC-rdf-primer-20040210/

[20] B. Parducci, H. Lockhart, and E. Rissanen, *eXtensible Access Control Markup Language (XACML) Version 3.0*, OASIS Std., August 2011.

[21] G. Karjoth, A. Schade, and E. V. Herreweghen, "Implementing ACL-Based Policies in XACML," in *Annual Computer Security Applications Conf. (ACSAC)*, December 2008, pp. 183–192.

[22] S. Harris and A. Seaborne, *SPARQL 1.1 Query Language*, W3C Std. [Online]. Available: http://www.w3.org/TR/2012/PR-sparql11-query-20121108/

[23] C. Floerkemeier, C. Roduner, and M. Lampe, "RFID Application Development with the Accada Middleware Platform," *IEEE Systems Journal, Special Issue on RFID Technology*, December 2007.

[24] K. Murthy and C. Robson, "A model-based comparative study of traceability systems," in *Proc. of the Int'l Conf. on Information Systems, Logistics and Supply Chain (ILS)*, May 2008, madison, Wisconsin.

[25] D. Corkill, "Blackboard systems," in *AI Expert*, no. 6(9), September 1991, pp. 40–47.

[26] R. Housley, W. Ford, W. Polk, and D. Solo, *RFC 2459 – Internet X.509 Public Key Infrastructure*, IEFT, Internet Engineering Task Force Std., January 1999. [Online]. Available: http://www.ietf.org/rfc/rfc2459.txt

[27] J. Schiefer, S. Rozsnyai, C. Rauscher, and G. Saurer, "Event-driven rules for sensing and responding to business situations," in *Proc. of the 2007 Inaugural Int'l Conf. on Distributed Event-Based Systems (DEBS)*. New York, NY, USA: ACM, 2007, pp. 198–205.

[28] D. Guinard, C. Floerkemeier, and S. Sarma, "Cloud computing, REST and Mashups to simplify RFID application development and deployment," in *Proc. of the 2nd Int'l Workshop on Web of Things (WoT)*. ACM, 2011, pp. 9:1–9:6.

[29] M. Linkies and F. Off, *SAP Security and Authorizations*. SAP Press, June 2006.

[30] R. Bhattacharyya, D. Deavours, C. Floerkemeier, and S. Sarma, "RFID Tag Antenna Based Temperature Sensing in the Frequency Domain," in *IEEE Int'l Conf. on RFID*, 2011, pp. 70–77.