AUTO–ID LABS

Improving the safety and security of the pharmaceutical supply chain

Learnings from the Drug Security Network

Mark Harrison and Tatsuya Inaba

Auto-ID Labs White Paper WP-BIZAPP-030

Mark Harrison
Senior Research Associate
University of Cambridge

Tatsuya Inaba
Research Associate
Keio University

Contact:

E-Mail: mark.harrison@cantab.net

Internet: www.autoidlabs.org

Business Processes & Applications

1. Introduction

This paper discusses various techniques that may be used to combat counterfeiting in the pharmaceutical supply chain. These include the use of electronic pedigrees (to ensure the integrity of the supply chain), together with mass-serialization (to provide for a unique lifecycle history of each individual package) and authentication of the product (to check for any discrepancies in the various attributes of the product and its packaging are as intended for that individual package). Management of the pedigree process and product authentication is discussed in some detail, together with various other learnings from the Drug Security Network, including identification of some remaining vulnerabilities and suggestions for tightening these loopholes.

2. The Drug Security Network

The Drug Security Network (DSN) was formed as a forum for a number of major players in the pharmaceutical industry to consider the major changes and challenges to business practices which will result from the enforcement of pedigree legislation [1] and introduction of mass-serialization, which are being introduced imminently in order to make the pharmaceutical supply chain safer and more secure.

The DSN was led by Cap Gemini and SupplyScape Corporation, with participation from GSK, Roche, Amerisource Bergen and members of Auto-ID Labs at MIT and Cambridge (UK), together with technical contributions from Hewlett-Packard and Verisign.

Unlike other initiatives such as Jumpstart, (led by Accenture), the focus of the DSN activity was not on creating or supporting an industrial field trial – but rather in developing pro-active thought leadership on three major issues – pedigree, serialization and data sharing and security.

The approach taken was to define, identify and prioritize supply chain use cases, using storyboarding, scripts and activity diagrams, to consider not only the processes which are required or impacted in meeting forthcoming regulations, but to go beyond that and consider what additional measures could be introduced to achieve a more safe and secure supply chain, then finally, consider other drivers which could add business value, both in terms of greater efficiency or protection of brand, product integrity and reputation.

Following an initial plenary kick-off meeting in December 2004, the members of the Drug Security Network met for three 2-day face-to-face meetings in January, March and May of 2005, using the Cap Gemini Accelerated Solutions Environment (ASE) to facilitate a large amount of clear thinking within each meeting. Furthermore, a practical DSN laboratory was set up at the Boston offices of Cap Gemini, to demonstrate an end-to-end practical example

of how electronic pedigree could be managed between a manufacturer, distributor, pharmacy and returns processing company.

The motivation of DSN was to undertake focussed brainstorming among major players in the pharmaceutical market, identify a number of the open issues which either need to achieve consensus or require further research, and to publish the output of the activity, also contributing it as input to regulatory bodies such as the U.S. Food and Drug Administration (FDA) and the U.S. Drug Enforcement Administration (DEA) and to standards development processes at EPCglobal and elsewhere.

The primary deliverables of the DSN activities consist of three papers:

The first paper [2] is entitled 'Serialization Options for Tracking of Pharmaceuticals using Radio-Frequency Identification', authored by Dr. Mark Harrison of Auto-ID Labs at Cambridge, UK.

A second paper [3] is entitled 'Technical Issues of Electronic Pedigree Inter-organizational Transactions', authored by Dr. Tatsuya Inaba, formerly of Auto-ID Labs at MIT, now with Auto-ID Labs at Keio University in Japan. This is summarized in Sections 5-6 of this paper.

The third paper [4] provided an overview of the DSN activities and a summary of the two other papers, as well as a discussion of many of the remaining open issues to be addressed.

3. Electronic Pedigree

The purpose of a pedigree is to provide legal proof of a secure chain of custody from the originator of the pharmaceutical package (usually the manufacturer or wholesaler) through to the organization that sells or dispenses the pharmaceuticals. Three key issues need to be considered:

Pedigree Data Content/Format

Pedigree Processing

Pedigree Transmission Mechanism

3.1. Data Content and Format

A number of key requirements can be identified for a standardized format for electronic pedigrees:

Completeness

It is in the best interests of everyone that a 'highest common multiple' pedigree format emerges, with the complete superset of information required by the various US state and

federal legislation, as well as any other information which may be required by traceability legislation in other countries, such as Belgium [5] and Italy [6, 7], where traceability initiatives have already begun.

Global Scope

It is also very important to maintain a global perspective rather than being US-centric. For example, rather than have a data field for the US National Drug Code (NDC), have one field for product code and another field for product code type, such that in the USA, the product code type may be set to 'NDC' – while it may be set to other values in other regions of the world, such as the AIC code for the drug, issued by the Italian Medicines Agency (AIFA).

Suitability for legal or government audit

The scope of the information present in the pedigree format should be carefully considered, since it will be a legal document. Information that is not required by legislation nor essential to the implementation of pedigree security should be contained in a separate information document or wrapper – but not in the individual pedigree document format.

Government agencies may require that pedigree information systems and pedigree management applications should be audited, to ensure the security of the information and to ensure that it is not possible to falsify, alter or delete the information which constitutes the legal pedigree document. In particular, it is very important that when the pedigree is stored in electronic format, that adequate provisions are made for data backup and recovery and that records which form part of a legal document cannot be modified or deleted within the legal lifespan of that document.

Integrity, Authentication and Non-Repudiation

Digital signatures [8] provide document integrity, authentication and non-repudiation. The authentication checks that the information has not been altered from that which was signed and that the signer signed the information. The signed content must include the original hash and a reference to the public key of the signer. This allows each transaction to be electronically authenticated by the recipient's system.

With some input and refinement from the Drug Security Network members, SupplyScape Corporation have proposed an Open Universal Pedigree Interchange Format [9]. This was subsequently contributed as an input to the EPCglobal Healthcare and Life Sciences Pedigree Task Force, together with other contributions of schema from Cyclone Commerce, Raining Data and Verisign. The result was a blend of all four contributions. In terms of data content, it provides not only a superset of what is required by state laws in Florida [10], California, etc. and by the National Association of Boards of Pharmacy, but also additional product information fields such as Item ID, Pedigree ID and Parent Pedigree ID and transaction information such as transaction type (sale/transfer/return), license state and other digital signature information (key information, signature information, meaning associated with signature, timestamp of signature). Furthermore, an Advance Pedigree Notice (APN) was proposed as a wrapper or envelope for transmitting a collection of pedigrees. The APN can also contain additional business data to be shared with the trading partner, while keeping the

business information segregated, so that it is neither mixed with regulatory data in the pedigree documents nor propagated further down the supply chain beyond the specific trading partner for whom it was intended. The APN therefore consists of three elements:

1. Order / Trading partner information
2. Shared Business Data
3. Pedigree Information (a collection of one or more pedigree documents)

3.2. Pedigree Processing

Processing of electronic pedigrees for pharmaceutical packages requires the following three steps as a minimum requirement:

1. Authentication of the pedigree, including verifying transactions for all previous custodians before the product arrives
2. Whe receiving product, verification that the incoming product matches the authenticated pedigree
3. When shipping product, sign the outgoing pedigree and transmit to the next custodian before shipping the product.

Figure 1 illustrates the various stages of pedigree processing for both receiving and shipping processes. It also indicates the responsibilities for manufacturers, distributors and retailers/pharmacies. The figure also indicates which of the DSN use cases represents each processing stage.

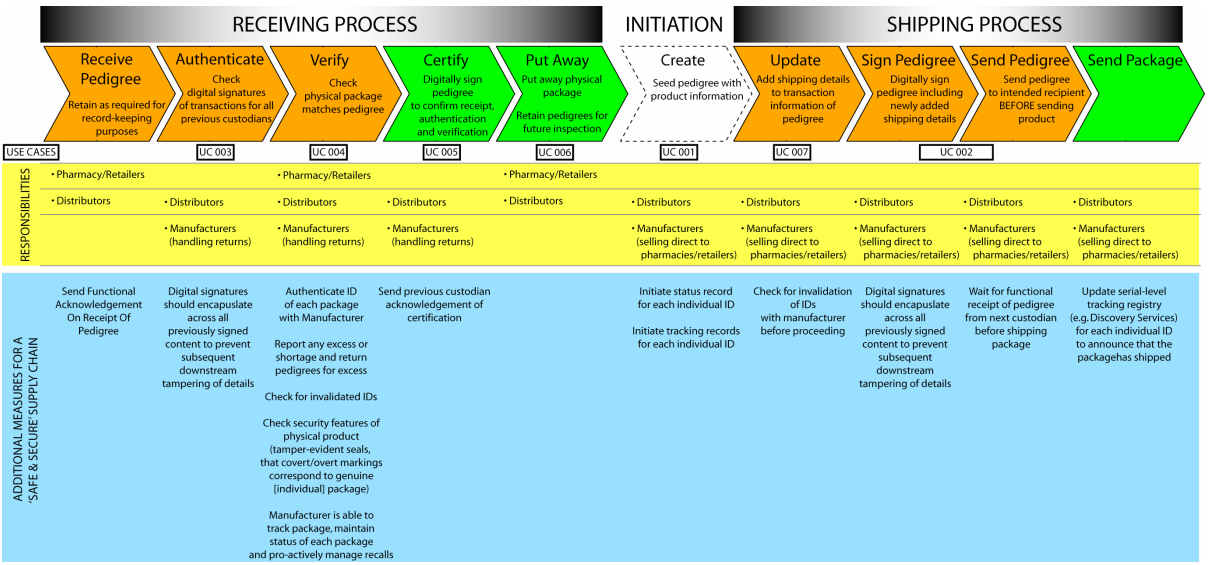


Figure 1 Stages of pedigree processing, roles and responsibilities and additional measures for a safe and secure supply chain

Figure 2 illustrates the stages of pedigree processing when additional measures are implemented to move closer towards a safe and secure supply chain, including various acknowledgement messages and potentially also updating of a serial-level tracking service such as the EPC Discovery Services in future. The acknowledgements and message choreography is discussed in much greater detail in the DSN paper by Dr. Tatsuya Inaba [3] , though Section 5 of this paper provides a summary of the paper.

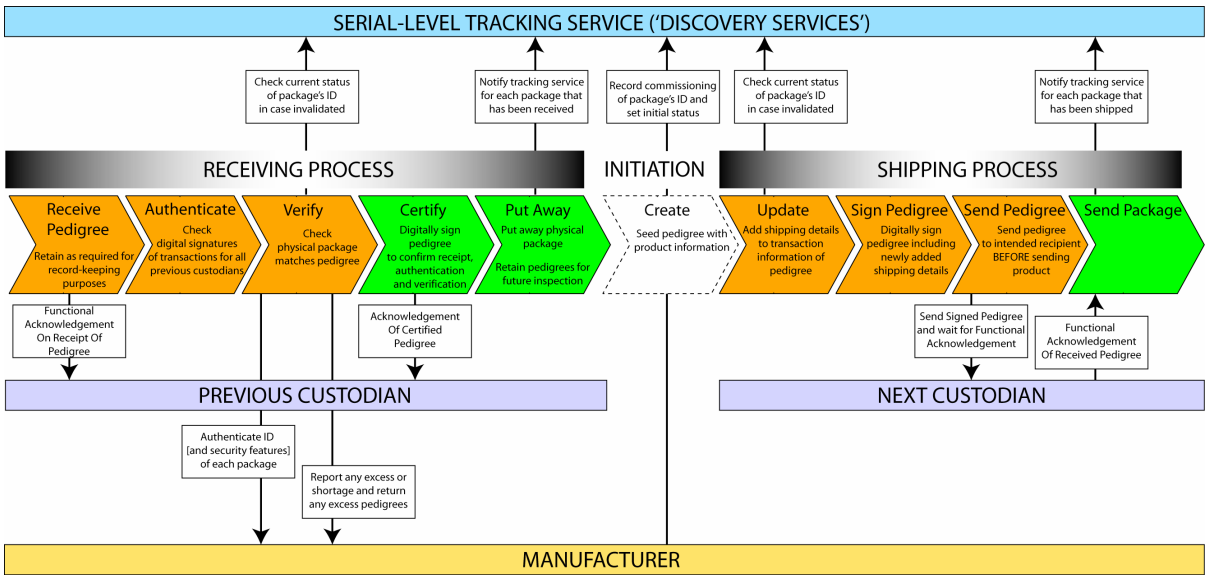


Figure 2. Stages of pedigree processing with enhancements to improve safety and security of the supply chain

It must be remembered that a pedigree is a document of record, which is subject to record-keeping, record retention and record availability requirements. Furthermore, electronic systems for managing pedigree documents are subject to regulatory requirements to provide computer systems security and control in order to protect against tampering with computers or electronic records.

It is optional whether manufacturers create and provide a pedigree to their customers, unless the manufacturer is selling direct to a retail store, in which case it needs to provide a pedigree. In 2005, the legislation in the USA did not require pharmacies and hospitals to authenticate received pedigrees, although they were required to retain them.

3.3. Pedigree Transmission Mechanism

A number of key requirements can be identified for the transmission mechanism for electronic pedigrees:

Timely access to data for verification and certification processes

It is essential for the efficient operation of business that verification of all previous custodians and transactions can take place rapidly, without significant network delays or outages.

Robust access to data for verification and certification processes

It is essential for the legal audit, that the verified trace of all previous custodians and transactions can be completely retrieved, whenever required, whether from a locally stored copy or from a distributed system of information services.

Authentication, Integrity and Non-Repudiation

The Pedigree format or Pedigree access mechanism should provide for the highest technically achievable degree of security to ensure that each successive custodian can authenticate the pedigree and verify the trace of previous custodians and transactions, as well as appending and certifying the pedigree information when they in turn propagate the pedigree with goods shipped downstream.

Suitability for legal/government audit

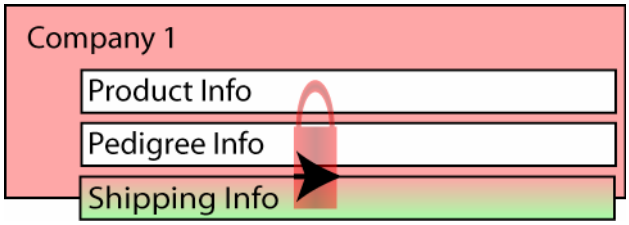
This may have an impact on the decision about how closely to integrate the pedigree into more general-purpose software, such as legacy EDI applications or the EPC Network [11, 12] components (specifically EPC Information Services), since doing so may result in these entire systems falling within the scope of government auditors.

There are two principal mechanisms by which pedigree information may be transmitted forwards down the supply chain and by which it may be subsequently retrieved. In the propagating document approach, the pedigree data is contained within a document, which is appended, re-signed and forwarded by each successive party in the supply chain. In the fragmented data approach, the pedigree data is stored separately by each party in their own information systems or those of a third-party provider, rather than being propagated down the supply chain. The relative merits of the two approaches are discussed below.

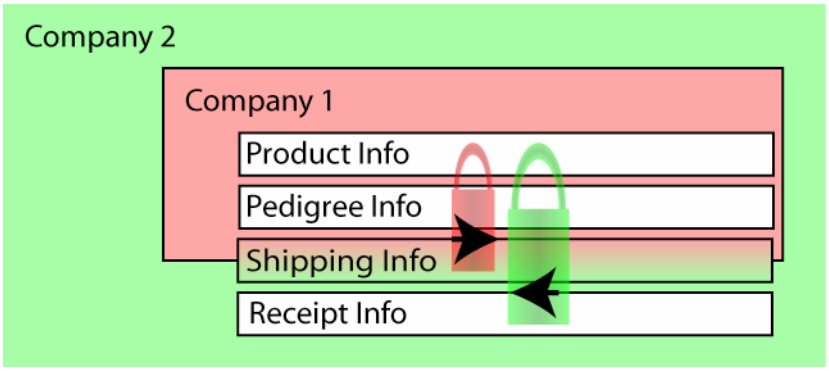
3.3.1. Propagating document approach

In this approach, each subsequent custodian verifies the signed content of previous custodians, then amends and re-signs the data, before transmitting the pedigree to the next custodian when the goods are shipped onwards. As the pedigree document moves across the supply chain, additional outer layers are added. As a consequence, the length of a propagating pedigree document can rapidly grow from a few kb to around 1Mb per consumer-level package if each ‘layer’ of the pedigree document includes a full digital signature.

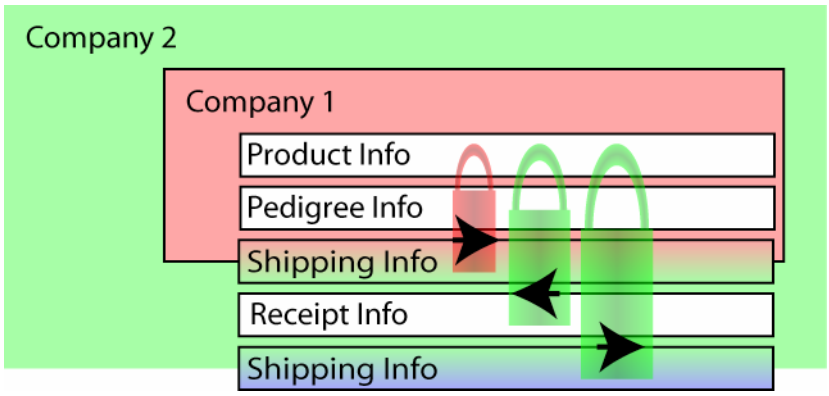
a)


Company 1
Product Info
Pedigree Info
Shipping Info

b)


Company 2
Company 1
Product Info
Pedigree Info
Shipping Info
Receipt Info

c)


Company 2
Company 1
Product Info
Pedigree Info
Shipping Info
Receipt Info
Shipping Info

d)

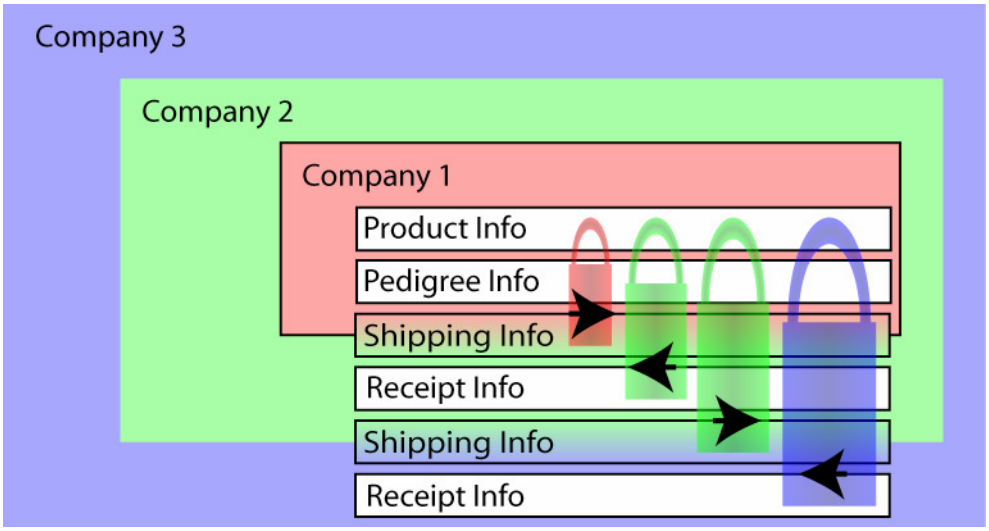


Figure 3. Propagating document transmission mechanism for pedigree. The padlocks represent a digital signature over the content indicated, effectively providing a tamper-evident lock against over-writing of the information over which the signature applies. Note that by signing both the shipping and receiving information, the method provides a double-linked secure chain of custody, as represented by the arrows.

This approach offers a double-linked chain of security, since each custodian can verify all the inner layers of the pedigree document, then signs to confirm that they have done so (the reverse link). At the time of shipping, they then add additional data about the next recipient and sign this (the forward link). The double-linked chain is intended to ensure that each successive custodian is the one whom the previous custodian intended as the next recipient of the package.

A further major security benefit of the propagating document approach is that as soon as the goods pass further down the supply chain, the despatching party no longer has complete control over all copies of the data, since all subsequent receiving parties will also obtain copies of the data. If the despatching party fails to produce the required data when requested to do so, there are other copies of the data in circulation further down the supply chain. As well as providing some additional robustness against accidental deletion, this approach also provides some protection against deliberate falsification of the records after the event, since a discrepancy with the data held by downstream recipients will be apparent upon investigation.

XML markup [13] is a standard method of communicating structured data in a way that is both human-readable and machine-readable and can be readily reformatted (e.g. using technologies such as XSLT) into alternative formats. The methodology of constructing digital signatures over parts of XML documents is already standardized by W3C [8].

3.3.1.1. Fragmented data approach

In this approach, the pedigree information is not sent forward from one custodian to the next. Instead, each company hosts its own electronic pedigree records on a networked database or information service, which is secured but to which trading partners and regulatory agencies are granted appropriate access.

Subsequent custodians are merely sent a hyperlink to the information, rather than being sent the data itself. This is shown schematically in Figure 4.

The obvious advantage is that much smaller amounts of data are being transmitted across the network, since the hyperlink is typically much smaller than the amount of data that it represents.

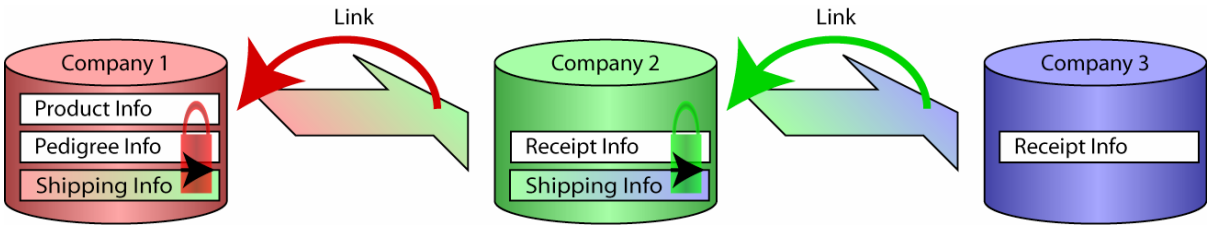


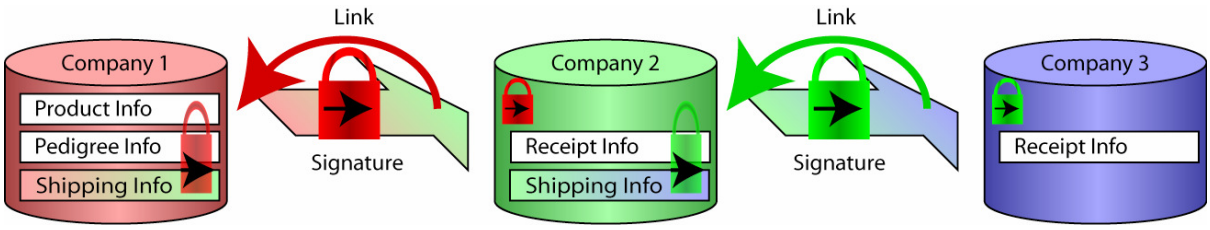
Figure 4. A simple fragmented data approach to linking of pedigree data. Each company sends the next custodian a link to the pedigree data they hold for the product but retain the data themselves rather than embedding into a pedigree document.

A potential disadvantage of this approach is that the receiver will need to contact each of the previous custodians independently in order to authenticate the package. This may actually result in an increased burden on the internet and local network and may halt the authentication stage if any of the upstream parties is temporarily unreachable, just because the full information required for authentication has not been transmitted in a self-contained way. Indeed, this type of distributed pedigree mechanism was discussed at the EPCglobal Healthcare and Life Sciences (HLS) meeting in Chicago – but it was considered that it did not meet robustness of available information because of the number of remote servers which needed to be contacted for verification and the cumulative probabilities of downtime over the set of relevant database servers. The buyers felt that the potential delays involved were unacceptable.

The major vulnerability in this approach is that potentially each company retains the only authoritative copy of their data – and would technically have the ability to either delete or amend and re-sign modified data, if the company were under investigation, even though such deletion or amendment and re-signing would be unlawful. A potential solution to this vulnerability would be for a requirement that when a company registers their involvement in the pedigree chain for a particular individually serialized package, they provide not only a network address to the data but also a digital signature of the data to the next receiver (see

Figure 5a) and/or to a central registry (see Figure 5b), to which they are granted only one-time write access for each individual package.

a)



b)

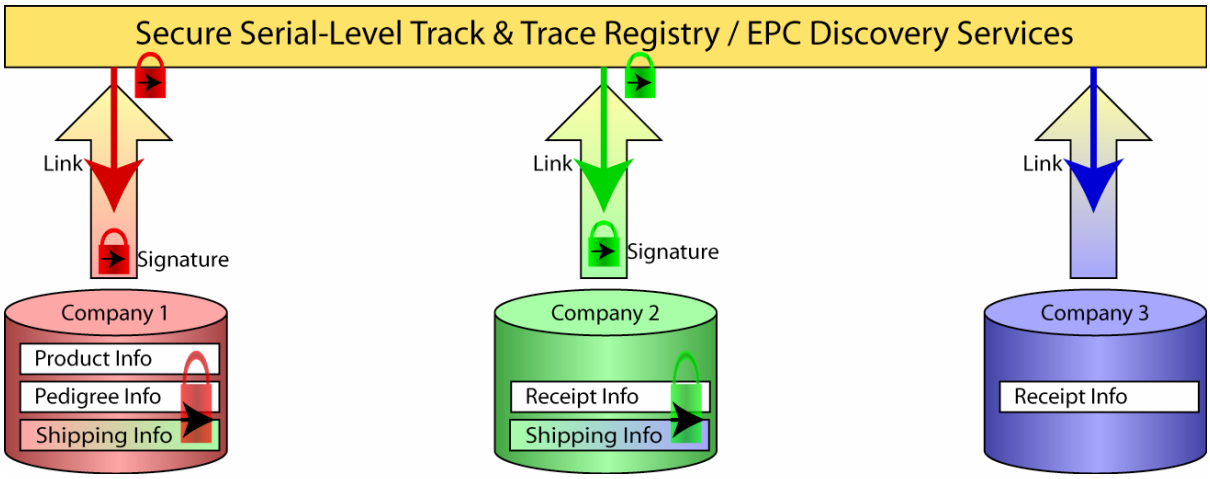


Figure 5. A more robust mechanism for linking distributed pedigree information. In (a), the link to the pedigree information is sent from the shipper to receiver and is accompanied by a digital signature, which is retained by the receiver. In (b), the link to the pedigree information is sent to a secure serial-level track and trace registry or EPC Discovery Service, together with a digital signature, which is retained by the registry; each company is only allowed one-time write access for posting the signature.

Even if the data they hold is subsequently falsified and re-signed, the new digital signature will not match the value that was transmitted to the receiver (and retained by the receiver) and/or stored earlier with the serial-level tracking registry. If the shipper sends a digital signature regarding their information to the receiver, then it is important that the receiver retains the digital signature they received in addition to any hyperlink information to the data,

since this independent digital signature may be required by government inspection if subsequent falsification of data by the shipper is suspected. The retention of received digital signatures is also shown in Figure 5a, 5b.

Figure 5b introduces the concept of Discovery Services or registries holding serial-level pointers to information across the supply chain. This approach raises a number of issues regarding administration, operation and financing of such registries, all issues which need to be seriously considered by the regulators.

If a distributed approach to pedigree management were implemented, the issues of both record loss and access delay would need to be fully considered in the architectural design.

4. Authentication of Identity and of Products

To the members of the Drug Security Network, pedigree is only one aspect of the safe and secure supply chain. It provides a legal trace of the chain of custody of a product. However, as well as being able to verify the custody history of a package, an equally important aspect is the ability to track where a package is at the current time, especially in a product recall scenario. Pedigree by itself does not provide this, since there is no current requirement for information to be sent back upstream in the supply chain, towards the manufacturers – only for the pedigree information to be passed downstream. Even then, a pedigree document primarily records a chain of transactions. It does not warrant that the package itself is the genuine product. For this, authentication is required. One can think of two kinds of authentication:

- authentication of the identity, since the identity provides the 1–1 link to the pedigree data
- authentication of the product itself, in case the identity of the package has been copied or the details about the product have been falsified

The manufacturer typically holds information about which identities or serial numbers have been ‘commissioned’ for genuine products they have released. This might also include correlations between the package ID and the original hard-coded ID built into an RFID tag, in order to make it more difficult for counterfeiters to simply copy the package ID onto duplicate RFID tags. The manufacturers also hold data about dates of manufacture, date of expiry and other information that may also be recorded in the pedigree document or printed on the label of the package. They might also retain records of any mass-customized specialized security features that were used for a particular serial number, as well as details of what tamper-evident seals or packaging should be expected.

A key feature of the Safe and Secure Supply Chain is the emphasis on authenticating the object, as well as the pedigree trail, as shown conceptually in Figure 6.

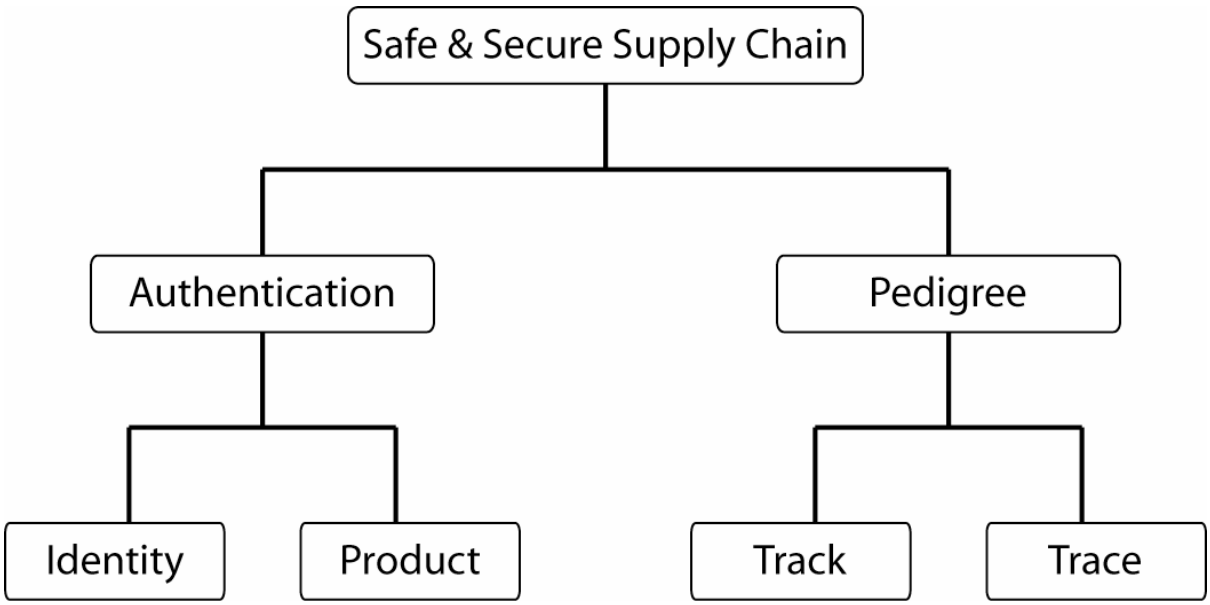


Figure 6. DSN concept diagram to illustrate the fundamental elements of a safe and secure supply chain.

If downstream supply chain parties authenticate the identity and product with the original manufacturers for each individual serialized package, then the manufacturers will gain much greater downstream visibility about the current locations of their products, which in turn should enable them to track them efficiently, if a recall needs to be triggered.

A networked information system, such as one complying with the future EPC Information Services (EPCIS) standard, would provide a mechanism for a manufacturer or labeller (or other authoritative party) to be able to validate a number of properties specific to a particular serial number. These might include an independent hard-coded read-only tag ID, the product class and/or details of customized security features, either covert or overt.

Clearly such information must only be provided to authenticated authorized parties, in order to prevent counterfeiters from abusing the system. In some cases, it may be practical or even preferable for the networked information system to simply respond with a Boolean (Yes/No, Pass/Fail) response to a challenge from an authenticated authorized client.

i.e. the system is allowed to respond to a query such as:

> 'Does this Tag ID / Product Type / Combination of security features correspond to this Object ID ?' (Answer is Yes or No)

but the following type of query might be forbidden to prevent counterfeiters from mining such a Product Authentication Service:

'Tell me the Tag ID / Product Type / Combination of security features for this Object ID'.

At present, one way in which this sort of Challenge / Boolean Response type query might be implemented in EPCIS is for the provider of the EPCIS service to allow access to a query whose input parameters are the Package ID or EPC and the Product Type or Combination of security features detected. An empty result set or a count of 0 events indicates no records – i.e. there is no match between the Package ID/EPC and the specified Product Type or security features – i.e. authentication failed, whereas a non-empty result set or a count of 1 event indicates successful authentication.

The pharmaceutical industry needs to consider whether this type of query approach is sufficient for object authentication purposes or whether custom types of query are needed – and whether there needs to be greater access controls regarding who is allowed to receive records of the 'commissioning event' when an EPC is first created for a package, since this event might normally hold details of attributes about the object, such as which Tag ID was used – or which combination of security features are present. i.e. when a pharmaceutical manufacturer implements an EPC Information Service, it may have its security controls configured to exclude the commissioning events from general EPCIS queries – and only provide them to a restricted group of clients and only when two or more parameters are supplied which match the commissioning event, i.e. only on a challenge-response basis.

When validating the authenticity of the product, it may be necessary to check the following criteria:

Authenticity of the tag

- Was the tag being read the same original tag which the original manufacturer or labeller applied? (i.,e. do the EPC and TagID match the manufacturer's records about the association between a particular Tag ID and the corresponding EPC?)

Authenticity of the pedigree ID

- Is the number of pedigree IDs greater than the number allowed for a given lot?
- What is the structure of the pedigree ID?
- Was the pedigree ID actually issued by the manufacturer or labeller?

Authenticity of the serialized identifier

- Is the serialized identifier or EPC programmed into the tag a valid one?
- Has that particular serialized identifier or EPC been issued by the manufacturer?
- Does the serialized ID or EPC match the one specified in the Pedigree?

Authenticity of the product's packaging

- Are there security features (microprinting, holograms, watermarks, iridescent inks, UV inks)?
- Have the security features been mass-customized (i.e. not always the same combination for all products or all serial numbers within a product line)?
- Do the information services have a record of the security features to expect (and where to find them) – and those not to expect? (which if present, indicate that the packaging is suspect)
- Does the mass-customization of security features (both present and absent) agree with what is observed?

Checking the current state

- Is that particular serialized identifier or EPC still available for distribution, sale or dispensing or has it already been decommissioned, marked as sold, recalled, returned, destroyed, etc.
- Is the information record corresponding to that serialized identifier or EPC now closed?
- Is the serialized object still in circulation beyond the expiry date assigned by the manufacturer?

Authenticating the trail

- Can the pedigree trail be verified for all previous custodians?
- Has the object followed a permissible supply chain path, without irregularities? (How can irregularities be defined?)
- Where are the events signifying cross-border transportation and customs clearance?
- Is the serialized object travelling along the forward supply chain or the reverse supply chain? Is this consistent with the last recorded state and intended destination region for that object? (What are the possible states and permitted state transitions?)

5. Data Sharing and Security

This section provides a summary of the DSN paper [3] entitled, 'Technical Issues of Electronic Pedigree Inter-organizational Transactions', authored by Dr. Tatsuya Inaba, Auto-ID Labs, (Keio, Japan), formerly at Auto-ID Labs (MIT)

The paper is primarily concerned about the messages that are exchanged between businesses in order to conduct transactions, once the requirements for pedigree are in force. The choreography of messages is documented in terms of Unified Modelling Language

(UML) [14] activity diagrams, together with tables of descriptions. Functional acknowledgements, transactions, timeouts and retries are also considered.

The paper also discusses various aspects of security, transport protocols and includes an analysis of the network bandwidth requirements which will be required for processing of electronic pedigrees and uses queuing theory to estimate the waiting times and number of items in queues to be processed.

5.1. Use Cases

Three groups of use cases are considered:

Base Case

- sufficient to comply with Florida pedigree law
- implemented in DSN Lab

Safe and Secure

- goes further, contains use cases useful in realizing the vision of a safer, more secure drug supply chain
- specifically identifies the following (currently optional) steps as being characteristics of a safe and secure supply chain:
- shipment confirmation messages,
- confirmation messages of the order from the buyer,
- termination or closure of the object's identifier and the associated pedigree document

Business Value

- realizing business value for companies employing an e-Pedigree application

Use cases are considered from an inter-organizational perspective, rather than an intra-organizational perspective. The use cases documented have clearly defined goals, scope/level, preconditions, description and successful end conditions and fail end conditions. Tables list the primary actors (described by roles (buyer/seller) rather than as manufacturer/wholesaler/retailer), triggers, frequency and extensions, issues and notes.

The paper clearly distinguishes between the different impacts of electronic pedigree on retailers and wholesalers / distributors; whereas wholesalers must receive goods from their suppliers and verify the pedigree, then authenticate and certify the pedigree document, before selling the goods, a retailer is only required to receive and verify, but is not currently

required to authenticate and certify the pedigree document, or to 'close' the pedigree document. This is illustrated in Figure 1 of this paper.

When mass-serialization is introduced, there will be significant changes to receiving processes:

- It will no longer be sufficient to check bulk quantities and product types against a purchase order.
- For each item, there will need to be a check for a 1–1 match of serial numbers between:
- Pedigree documents with purchase order
- Pedigree documents and received items

A further complication is that the buyer might not necessarily receive all pedigree documents at the same time, even though the buyer also needs to control the relation between pedigree documents and purchase orders.

The paper considers the message choreography in terms of the following:

- Offer documents (e.g. Purchase Orders (PO), Shipping Notices)
- Acceptance documents (response to offer – need not be electronic)
- Functional acknowledgements (a message from seller to verify syntax or confirm correct transmission/format, not necessarily acceptance of deal)

The timing between messages, acceptable delays and time lapses before retries are acknowledged is an issue which must be considered and may have impacts on the design of e-pedigree application software, although the actual policies and actual values of time to retry, number of retries etc. are matters for trading partners to agree upon. Many of these parameters are already handled in existing EDI standards, such as the X12 series [15] – but pedigree management software will need to be able to be configurable with these policies, ideally in a machine-readable way. The paper also considers revocation documents used to cancel an offer document before an acceptance document is received.

5.2. Security

In the discussion on security, the paper [3] identifies five key security requirements:

Authentication
– establishes trust regarding the identity of two partners exchanging messages

Authorization
– does the other partner have appropriate authorization to send a business document / deal?

Confidentiality
– is the communication channel private? (e.g. encrypted documents / channel)

Integrity
– is it certain that the business document is not garbled or tampered?

Non-Repudiation
– receiving partner has proof of the receipt of the original business document – and the initiating partner has a proof of the receipt that the receiving partner successfully received the business document.

The paper then discusses how specific existing EDI and internet technologies can be used to cover each of these aspects of security. These are summarised in the table below.

Technology solution	Security feature offered
EDI-INT AS2 + SSL + S/MIME	Partner authentication and authorization
SSL + S/MIME	Confidentiality of message exchange
Digital Signature embedded in S/MIME packet	Data integrity and non-repudiation of the original business document
Message Disposition Notification (MDN) sent back from receiver to initiator	Non-repudiation of message receipt
Public Key Infrastructure (PKI) + Digital Signatures	Guarantee authorization of the business document

5.3. Pedigree documents - Information content

The concept of a Pedigree Business Document is introduced. This serves as a wrapper or envelope to consolidate several individual pedigree documents when multiple packages are shipped together. However, the individual pedigree documents remain intact within the Pedigree Business Document, which makes it easier to send them forward when shipments are split further downstream.

The format of the individual pedigree document could either be a common format agreed by all states – or a composite of the separate pedigree formats that individual states decide to use, which contains a superset of all the information which is required, even if some of it is not required by each state.

Information in the pedigree document includes:

- Information which is unique to a particular pedigree document (ID, version of format, timestamp)
- Information which is unique to an individual product package (Drug name, Manufacturer/Distributor, Object ID, NDC, Manufacturing date, Expiry date, Dosage form, strength, container size, lot number, parent package object ID)

When the package is about to be sold or transferred to the next custodian, the following is added:

- Information about the shipper
- Transaction data (sales invoice no, date of purchase, quantity by lot number)
- Shipper information (business name, address, licence number, name, title, address of person certifying pedigree, timestamp of signature, meaning of signature etc.)

The shipper then digitally signs the pedigree.

Upon receipt, the receiver validates the digital signatures (authentication) and after matching received products with the pedigree document (verification) then signs the pedigree to confirm receipt (certification). At this point, the packages can be put away until needed.

When the receiving party is ready to dispatch the packages, they take on the role of the shipper and append the pedigree with:

- Information about the shipper
- Transaction data (sales invoice no, date of purchase, quantity by lot number)
- Shipper information (business name, address, licence number, name, title, address of person certifying pedigree, timestamp of signature, meaning of signature etc.)

Finally, they digitally sign the Pedigree documents and send the pedigree information in advance of sending the package.

These processing stages are also shown schematically in Figure 1 of this paper.

The paper also considers the following pedigree-related documents or messages:

- Pedigree Document Acceptance – also considered as a type of pedigree document, with a similar structure
- Revocation document – refers to original offer document – but does not contain pedigree info.
- Functional acknowledgement – generic, refers to original document, plus status and reason for error.
- Pedigree business document – wrapper to carry multiple pedigree documents and related business info. This may be either an Advance Pedigree Notice or a Pedigree document acceptance.

The paper also includes a comparison of how e-business technologies such as AS1 [16], AS2 [17] and AS3 and ebMS [18] can handle security aspects (confidentiality, integrity, authentication, authorization, non-repudiation), functional acknowledgement, revocations, retries, payload types and synchronous vs asynchronous communication. The paper [3] also provides a comparison of the AS1/AS2/AS3 specifications used in e-business.

5.4. Other issues

The problem of managing identifiers is not overlooked; the paper identifies the need to maintain associations between Purchase Order (PO) numbers and the number of the Advance Pedigree Notice (APN) – and between the Advance Pedigree Notice (APN) and the Advance Shipping Notice (ASN), in the case where an ASN is used. It is expected that the Advance Pedigree Notice would list the unique serialized IDs of each package. This highlights a problem when no ASN is sent; the buyer does not have advance notice of which shipment contains which order or pedigree.

A section of the paper also considers use cases for Less-Than-Truckload (LTL) (e.g. consolidated shipments of mixed cases). The use case involving third-party carriers is also considered.

The paper also discusses how wholesalers could use an Advance Shipping Notice to construct a pedigree document.

Appendix F of the paper considers the following use cases:

- Normal Buyer/Seller in response to purchase order
- Vendor managed inventory
- Handling returns, handling chargebacks / proof of sales

There will be a need to not only design new documents such as Pedigree document and Pedigreee business document (wrapper/envelope) – but also assess the impact of the Pedigree application on existing inter-organizational transaction standards, specifically in terms of links with the pedigree documents.

5.5. Risks of paper pedigree

Appendix G of the paper [3] discusses the use of paper-based pedigree from wholesaler to retailer, to cope with retailers who cannot receive electronic messages, authenticate electronic Pedigree documents – or read object identifiers. Although this practice is currently allowed, it carries the following risks:

- Lack of digital signature technology. As discussed in section 6 of this paper, in comparison with handwritten signatures, digital signatures provide a much higher level of confidence that the data was not corrupted or tampered with – and that the digital signature was not forged by someone else.
- Retailers cannot authenticate all the previous digital signatures of previous trades and handovers, nor the authenticity of the paper itself. Wholesalers may need to use overt anti-counterfeit measures to the paper-based Pedigree document.

- Retailers cannot check the authenticity (trade history) of the product before the product is shipped from wholesalers. Wholesalers may not execute granular status control without confirmation messages from retailers.
- Retailers can only verify received products by counting number of items and number of paper-based Pedigree documents. Human-readable object identifiers on the items and the paper-based Pedigree documents are necessary to verify the shipment. This may be quite labour intensive.
- Retailers may need to use handwritten signatures – but these do not have robust verification mechanisms, so once Pedigree document is printed out rather than being handled electronically, the pedigree (and the associated drug package) is not transferable (or has a potential risk of counterfeiting). This may also impact the legitimate returns process.
- Retailers do not terminate the object identifiers and associated Pedigree documents when the packages are dispensed. Even if they can terminate the pedigree, paper-based Pedigree documents may be illegally reused assuming that some of the retailers just count the number of both drug packages and papers without checking the object identifiers.

The paper identifies a number of potential loopholes of paper-based pedigree documents:

- Wholesalers can print out paper-based pedigree documents of items sold to retailers with electronic pedigree – or sold to other retailers with paper-based pedigree documents. Wholesaler can have more paper-based pedigree documents than saleable items. Then, a fraudulent wholesaler can sell counterfeit items with legitimate paper-based Pedigree documents.
- Retailers can sell paper-based Pedigree documents to wholesalers. Retailers may be able to sell the object identifiers with paper-based Pedigree documents to a wholesaler. A fraudulent wholesaler may forge paper-based Pedigree documents and sell counterfeit items saying they are returns from the retailer.

In summary, using paper-based Pedigree documents increases the risks of entry of counterfeit drugs. One of the major issues here is that those who receive paper-based Pedigree documents cannot validate the trade history of the items, which is a purpose of implementing electronic Pedigree application. This also means that once a Pedigree document is printed out, the item should be transferred in the limited area. If it is allowed to re-convert paper-based Pedigree document into electronic Pedigree document, the next buyer should be notified of the risk associated with the products.

The paper also considers conversion between different transport protocols – and the need to ensure that also errors and functional acknowledgements are correctly translated between protocols.

One must also consider the legal issue of intermediate companies – is confidentiality guaranteed? Does the intermediate company also assume liability for the transaction?

Are third party logistics companies also expected to comply with regulations?

6. Vulnerabilities

There are still a number of potential loopholes in the security of the proposed pedigree legislation. Regulatory bodies such as the FDA or DEA may be advised to review the vulnerabilities identified here and consider whether further guidelines or legislation needs to be issued.

6.1. Pedigrees initiated by the wholesaler rather than the manufacturer

In the USA, it is current practice for distributors to break down bulk product from manufacturers into smaller packages for shipment to retailers. In addition to the potential risks associated with paper pedigrees, there is the need for some clarification about how repackaged products should be identified and who is responsible for them. When mass serialization is introduced, it would be inappropriate for the distributor to re-use the serialized identifier of the bulk product for each of the smaller packages broken down from it, since each needs to be uniquely identifiable. Having said that, the pedigree record needs to provide the traceability all the way back to the source, so it should at minimum record the identity of the bulk product. Ideally, a new pedigree document should be created for a new package ID, which includes and extends the pedigree of the bulk product from which it was obtained. The new package ID may also be used for lookup purposes, to find authoritative information services about the package. There may be a legal issue about whether the distributor or the original manufacturer is the authority for that package and accepts the liability that accompanies this role. It is likely that wholesalers or distributors would only accept the liability and workload of applying RFID tags only for repackaged items – and in this case, the package ID should probably indicate the wholesaler or distributor, rather than the original manufacturer Finally, if it is allowed to use the original manufacturer's labeller code for the new package ID, there must be close co-ordination between distributor and manufacturer about allocation of serial numbers, in order to ensure that the manufacturer 'commissions' that particular serial number for that particular product class and records that it is a valid serial number, i.e. one which they have allocated. Ultimately, the organization that is the authority for the package ID (in this example, the manufacturer) would also be responsible for keeping track of when the package ID is ultimately decommissioned or 'closed', e.g. on dispensing, return or invalidation.

6.2. No requirement for closure – of the pedigree record or the serialized ID

At the point of sale or dispensing, when the package reaches the end of its normal supply chain, it is advisable to require that the corresponding pedigree document should be formally 'closed' or 'terminated' in order to avoid any opportunity of genuine pedigree documents recirculating to provide an alibi for counterfeit products being introduced into the supply chain.

By the same reasoning, it is also advisable for an authoritative record of the serialized ID to be formally 'closed' or 'terminated'. This does not mean deletion of records tied to that serialized ID – but rather that termination or closure should trigger an alert if the serialized ID is subsequently detected in the normal forward supply chain, since this may be an indication of a counterfeiter attempting to reuse discarded genuine packaging or serialized IDs read from genuine packaging to introduce counterfeit product. Within the architecture of the EPC Network [10], appropriate places to record 'closure' or 'termination' of an individual serialized ID are either in the EPC Information Service provided by the manufacturer or labeller – or as a 'flag' or field in the appropriate 'EPC Discovery Service' for the records for that individual serialized ID.

However, it is unlikely that most retail pharmacies would ever install the necessary infrastructure and staff training for closing out each serialized ID unless there is a legislative mandate requiring them to do so.

6.3. Conversion of paper pedigrees to electronic pedigrees

Digital signatures provide a much higher degree of security than handwritten signatures, since they are much more difficult to fake. A digital signature is essentially constructed from the data to be signed by algorithmically computing a message digest or summary of the data, then encrypting this with the signer's private key. In this way, the signature is different for each block of data, whereas a handwritten signature is expected to be approximately the same for each block of data. A change to a single bit of the data results in a completely different signature. Furthermore, because the signature is encrypted using the signer's private key, it is possible for anyone to use the signer's public key to verify that only they could have signed it – i.e. it provides a high degree of non-repudiation, so long as the private key is kept confidential. Knowledge of the signer's public key does not allow a third party to reverse engineer the signer's private key (at least not on a practical timescale with computing technology available today or in the near future) – so they cannot forge the signer's digital signature over data which they falsify.

Because handwritten signatures are easily forged and are not inextricably tied to the data being signed, there is a vulnerability if a pedigree in paper format (using a handwritten

signature) is ever allowed to be converted back into electronic format, because the handwritten signature offers a much lower guarantee of authenticity.

Pedigree documents in which any of the signatures is not entirely digital should not be regarded as first-class genuine electronic pedigree documents and the conversion of electronic pedigrees to paper formats should be avoided if at all possible – and ideally, pedigree legislation should dictate that paper pedigrees are not acceptable. Indeed, the pedigree legislation in California does not allow for paper pedigrees, even though the state of Florida does allow for both to co-exist. In practice, paper pedigrees are unworkable because of the high volumes of units involved at item-level and the way in which products are broken down into single unit quantities, which are then combined for distribution purposes.

However, a theoretically possible transmission of an electronic pedigree via paper is described below,

- An entirely electronic pedigree document is printed out or faxed onto paper.
- The recipient scans the document and performs optical character recognition (OCR) to regenerate the text file that was originally sent.
- The text file should be canonicalized, to ensure that no additional white spaces or line break characters have been inadvertently introduced and to eliminate any syntactic variability in how an XML document is formatted. W3C has already specified how to represent an XML document in canonical form [19].
- All previous digital signatures must be verified successfully. If any of these fail, then there may be an error in the OCR process or the canonicalization. Return to step 2.
- At this stage, the recipient is effectively in possession of an electronic pedigree document and should then sign, add the shipping information, then re-sign.

This approach is not recommended in practice for normal operations, since it is clearly very time consuming and inefficient to scan and perform optical character recognition to reconstruct the XML document. Furthermore, this approach is only applicable between immediate nearest neighbour trading partners within the supply chain. It is not possible to reconstruct a secure first-class XML electronic pedigree if a handwritten signature has been included while the pedigree was being transmitted via paper.

In practice, once pedigree legislation is fully in effect, it is much more advisable for companies to implement a fully electronic pedigree management system and also to ensure that they (and their trading partners) have reliable network connectivity between them, with sufficient redundancy (e.g. via pre-positioning and local caching of data and possibly also the use of secondary internet service providers for backup) to ensure that the pedigrees conform to the highest available security, while also ensuring that their distribution/processing operations do not experience any downtime due to network connectivity outages.

If at any stage, any of the digital signatures fails to verify – or if any exchange is accompanied only by a handwritten signature, rather than a digital signature, then the pedigree can no longer be regarded as a first-class electronic pedigree for security purposes.

The current EPCglobal standard for pedigree allows for conversion from electronic pedigree to paper, although the paper signatures would simply serve a notice that the electronic signatures had been validated prior to printing. Further validation would require considerable manual methods allowed by law (e.g. e-mails, phone calls, etc.), all of which are considerably more time-consuming and labour-intensive than automated validation of electronic signatures.

6.4. The need for certification authorities

Certification authorities such as Verisign, Thawte and TRUSTe already act as trusted third parties who issue digital certificates that vouch for the correspondence between an individual or organization and their public key. This is routinely used for electronic commerce on the internet.

For electronic pedigrees for pharmaceutical packages, the public/private key is required to belong to a named individual within the organization, rather than belonging to the organization itself. It may also be appropriate to require that the certificate should contain the individual's licence number as approved by the relevant government agency for pharmaceuticals, e.g. US FDA. In this case, a standard web-trader digital certificate may not be acceptable – instead the government agency may require that certification authorities verify additional data such as licence number etc.

Some government agencies may even consider very close involvement in the process. Indeed, the Florida regulations on certificate authorities for self-authenticating pedigrees[20] impose many additional requirements beyond those that are usual for certificate authorities issuing certificates for ordinary e-commerce purposes.

6.5. Enforcing a change of serial ID and labeller code on repackaging

When a pharmaceutical package is broken down into smaller packages, it is essential that new serial IDs are created for each of the sub-packages, so that each is independently traceable for pedigree purposes. The new serial IDs should reflect the labeller code of the distributor, rather than the labeller code of the original manufacturer of the bulk product unless there is agreement and communication between the distributor and manufacturer about which serial IDs should be allocated, in order to ensure that the new serial IDs of the sub-packages can be correctly resolved to the appropriate information records.

6.6. Cross-border shipments and diversion

Diversion is a major issue for the retail sector, but even more so for the pharmaceutical industry, since pharmaceuticals are sometimes sold to developing countries at a discounted price compared with the prices charged to the developed world. Unfortunately, these pharmaceuticals often fail to reach those in developing countries who so desperately need medical treatment. Instead, they are often intercepted by criminals or corrupt regimes and re-exported to the developed world, for sale at the regular price, resulting in a profit for the criminals or corrupt regimes involved, at the expense of the people suffering in the developing countries as well as a financial fraud perpetrated on the pharmaceutical industry.

Effective pedigree records provide an opportunity to greatly reduce such diversion activities, provided that the pedigree includes details of cross-border shipments, including details of export licences, customs clearance, etc.

The pedigrees for pharmaceuticals that are intended for shipment to developing countries should perhaps contain information about the country or at least regions[1] of the world in which they are intended for use. This designation should be irrevocable in the sense that customs clearance officials should be actively involved in the pedigree process and required to check that re-importation is not taking place for discounted pharmaceuticals intended for a developing country or region.

If region-specific restrictions can be applied to consumer products such as DVDs primarily for the commercial purposes of market fragmentation, then surely a similar mechanism could be used for the far more worthwhile purpose of ensuring that pharmaceuticals which are intended for developing countries actually reach the people whose suffering could be alleviated by those pharmaceuticals and finally put an end to interception and diversion activities by criminals and corrupt regimes in those countries.

[1] For example, the United Nations International Strategy for Disaster Reduction has classified the world into three regions, not on a geographic basis – but in terms of economic development. See http://www.unisdr.org/disaster-statistics/pdf/Classification-countries-UNDP-report-2004.pdf

Acknowledgments

The authors wish to thank the reviewers from Cardinal Health and Cyclone Commerce for additional insights and recent updates, which have now been included within this paper.

References

[1] *The Prescription Drug Marketing Act: Report to Congress*. [cited; Available from: http://www.fda.gov/oc/pdma/report2001/default.htm.

[2] Harrison, M.G., *Serialization Options for Tracking of Pharmaceuticals using Radio-Frequency Identification*, in *Drug Security Network - White Papers*. 2005.

[3] Inaba, T., *Technical Issues of Electronic Pedigree Inter-organizational Transactions*, in *Drug Security Network - White Papers*. 2005.

[4] Harrison, M.G., *The Drug Security Network - An Overview and Discussion of Remaining Issues*, in *Drug Security Network - White papers*. 2005.

[5] *Royal decree modifying the royal decree of 21 December 2001 laying down the procedures, deadlines and conditions for intervention by the obligatory insurance for health care and benefits in the cost of proprietary medicinal products. (Kingdom of Belgium)*. 2003.

[6] *Bollini Legislation (Law 39 - 1st March 2002 (art. 40), Republic of Italy)*. 2002.

[7] *Bollini Legislation (Law 14 - 3rd February 2003, Republic of Italy)*. 2003.

[8] *XML and Digital Signatures*. http://www.w3.org/Signature/

[9] *Open Universal Electronic Pedigree Interchange Format*. 2005 [cited; Available from: http://www.epedigree.org.

[10] *Florida Prescription Drug Protection Act*. 2003. http://election.dos.state.fl.us/laws/03laws/ch_2003-155.pdf

[11] *EPCglobal Network*. See the Auto-ID Centre white papers at http://www.autoidlabs.org/whitepapers and EPCglobal Architecture Framework v1.0 at http://www.epcglobalinc.org/standards_technology/specifications.html

[12] *EPCglobal Architecture Framework Version 1.0*. http://www.epcglobalinc.org - see under 'Standards and Specifications'

[13] *XML - Extensible Markup Language*, W3C - World Wide Web Consortium. http://www.w3.org/XML

[14] *Unified Modelling Language (UML)*. [cited; Available from: http://www.uml.org/.

[15] The Accredited Standards Committee (ASC) X12.

[16] Harding, T., R. Drummond, and C. Shih, *MIME-based Secure Peer-to-Peer Business Data Interchange over the Internet*, in *RFC*. 2002, IETF - Internet Engineering Task Force. http://www.ietf.org/rfc/rfc3335.txt

[17] Moberg, D. and R. Drummond, *MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)*, in *RFC*. 2005, IETF - Internet Engineering Task Force. http://www.ietf.org/rfc/rfc4130.txt

[18] *ebXML Messaging Service*, OASIS - Organization for the Advancement of Structured Information Standards. http://www.oasis-open.org/committees/ebxml-msg/

[19] *Canonical XML Version 1.0*, W3C. http://www.w3.org/TR/xml-c14n

[20] *Certification Authority and Digitial Signatures for Self-Authenticating Pedigree*. 2006, Florida Department of Health (in Florida Administative Weekly, 2 June 2006).