AERO-ID

AUTO-ID LABS

Electronic Pedigree and Authentication Issues for Aerospace Part Tracking

Mark Harrison, Andy Shaw

Auto-ID Lab, University of Cambridge, UK

This report introduces electronic pedigree and authentication issues for aerospace parts tracking and draws upon insights from the activities of the Drug Security Network (DSN), which was formed to consider how to make the pharmaceutical supply chain safer and more secure.

The report provides a summary of the main findings of the DSN study and also a discussion of the remaining issues and vulnerabilities that still need to be considered by regulatory bodies, manufacturers, distributors, MROs, research organizations, standards bodies and technology solution providers.

The report goes on to propose research areas that need to be addressed, activities to be undertaken by standards bodies, opportunities for technology vendors and actions needed from the regulatory bodies.

The outputs from the proposed research would be in the form of supply network models, reports and detailed recommendations.

Published February 1, 2006. Distribution restricted to Sponsors until August 1, 2006

Table of Contents

Published February 1, 2006. Distribution restricted to Sponsors until August 1, 2006

1. Introduction

For a maintenance and repair organisation to be able to show that the replacement part that they are about to fit to an aircraft is genuine and carries the appropriate certification and approvals is critical in providing the quality of service required to keep aircraft flying safely and legally. The introduction of automatically readable unique identification technologies such as RFID provides the opportunity to transfer this burden of component data from paper to electronic media.

Here it is necessary to introduce two definitions. The first is “pedigree” which is the history of a part from its manufacture to its eventual disposal. Exactly what data is required to form this pedigree is a research topic in its own right but whatever is included needs to enable the verification of the truth of this history. This verification process is the second definition required and is called authentication. The automatic creation of pedigree and authentication information as parts are manufactured and progress through the supply network and repeated repair cycles helps to identify the life left in the component and inform decisions on its use.

In order to achieve widespread automated ID deployment for aerospace parts throughout the supply network, a common understanding of the concepts and issues surrounding pedigree and authentication has to be developed. Only on this basis can the actors in the supply network specify and contribute to the development of standards.

It is important to recognise that a pedigree document, paper or electronic, primarily records a chain of transactions. It does not warrant that the part itself is the genuine authorized part. For this, the further process of authentication is required, which ties the unique identity of a part to a pedigree record. In line with this analysis the concept of a custodian is introduced as being a supply network actor responsible for a part or component and its authenticity for a fixed period or periods during its life.

The aim of this report is to examine problems such as the transfer of pedigree and authentication processes from paper to electronic media and to identify areas where future research work is required. It draws extensively on the work carried out by the Drug Security Network (DSN) to create a more secure pharmaceutical supply chain. Outline details of the DSN project can be found in appendix 1.

Key research challenges identified in this project are identifying the data required for pedigree records on aerospace parts, data volume management, scaleable enhanced look up services and improved access control to tag data. Unlike pharmaceuticals aerospace parts have a long life and may be re-used and re-circulated through the supply network many times. This will generate large volumes of pedigree data per part. There are also ‘end of life’ issues here. With these increased data volumes comes the need for improved look-up services. If more data can be stored on the tag and new techniques are developed to control access then it may be possible to distribute the data around the network and diminish the need for enhanced look up services (cf Data Synchronisation issues).

Over the next twelve months we propose:

Published February 1, 2006. Distribution restricted to Sponsors until August 1, 2006

- The development of a comprehensive model of the controlled part supply network which can be part centric, actor centric or aircraft centric;
- Investigation of specific data management technologies;
- A review of current and future electronic security measures.

The outputs from this work would be in the form of models, reports and detailed recommendations. We anticipate extensive involvement from the end user community in creating the models underpinning the work on data volume management and from the technology vendors and standards communities in the other two areas.

This report first introduces in section 2 the concepts of pedigree and authentication and how pedigree data can be generated and managed using experience from work undertaken by the DSN. It brings together the findings from three DSN reports, [1], [2] and [3], and examines them in the light of the aerospace parts supply network. It goes on in section 3 to examine pedigree in detail and the requirements for the associated serialisation system and then discusses technical issues of pedigree transactions.

Section 4 examines potential vulnerabilities to security in the proposal for the pharmaceutical sector and how these could affect the aerospace part supply network. Section 5 outlines potential next steps for the aerospace sector and section 6 makes recommendations for further work in terms of research and development, standards, technology providers and regulatory bodies.

Published February 1, 2006. Distribution restricted to Sponsors until August 1, 2006

2. Pedigree processing

2.1 Authentication and Pedigree

In order to ensure that there was no confusion over terminology, the DSN members developed the tree diagram shown in Figure 1.

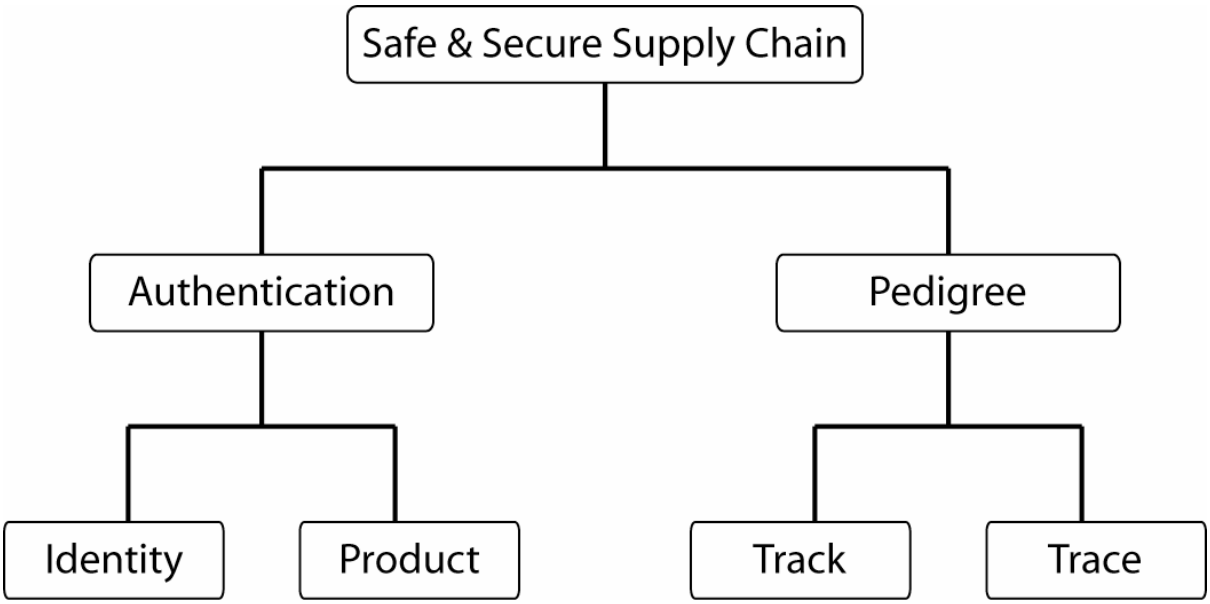


Figure 1 – DSN concept diagram to illustrate the fundamental elements of a safe and secure supply chain.

Pedigree is only one aspect of the safe and secure supply chain. It provides a legal trace of the chain of custody of a part. 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 part 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 part itself is the genuine authorized part. For this, authentication is required. One can think of two kinds of authentication:

1. Authentication of the identity, since the identity provides the 1–1 link to the pedigree data
2. Authentication of the part itself and its pedigree, in case the identity of the part has been copied or the details about the part have been falsified

The part manufacturer typically holds information about which identities or serial numbers have been 'commissioned' for genuine authorized parts they have released. This might also

Published February 1, 2006. Distribution restricted to Sponsors until August 1, 2006

include correlations between the part 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 part ID onto duplicate RFID tags. The manufacturers also hold data about dates of manufacture, data about expected lifetime / duty cycles of the part and other information that may also be recorded in the pedigree document or printed on the label of the part. 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, particularly where these have been applied to authorized parts which have been checked that they are fit for use. Appendix 2 of this report lists a number of the criteria that may need to be checked to authenticate the part.

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

2.2. Pedigree requirements

Considering the data requirements for electronic pedigree, these may include:

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

Figure 2 illustrates the various stages of pedigree processing for both receiving and shipping processes. It also indicates the responsibilities for manufacturers, distributors and receivers of parts.

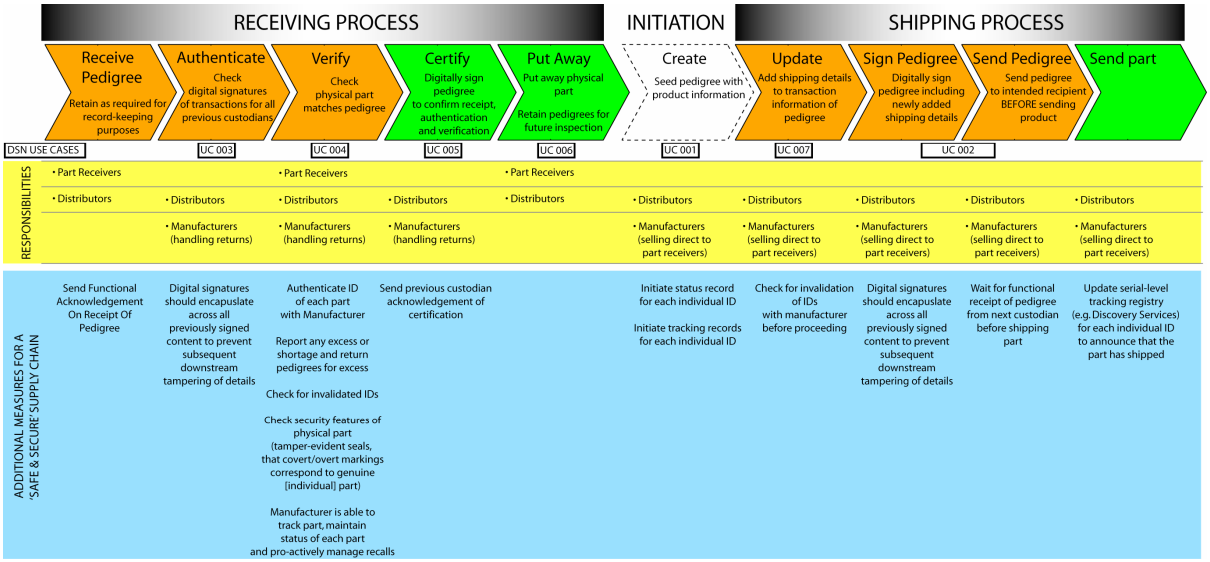
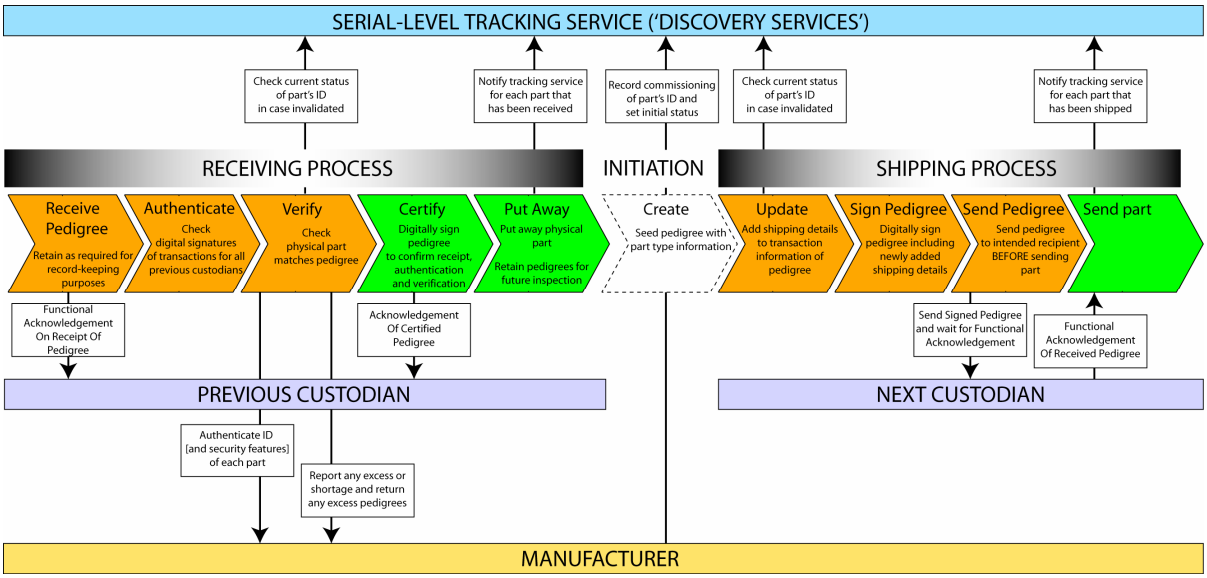


Figure 2 - Stages of pedigree processing, roles and responsibilities and additional measures for a safe and secure supply chain

Figure 3 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 second DSN paper by Dr. Tatsuya Inaba [2]. Section 3.3 of this report provides a summary of the key issues discussed in the paper.



Published February 1, 2006. Distribution restricted to Sponsors until August 1, 2006

Figure 3 – 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.

Digital signatures 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 signatory actually signed the information. The signed content must include the original hash and a reference to the public key. This allows each transaction to be electronically authenticated by the recipient's system.

It may be useful for the aerospace sector to review the Open Universal Pedigree Interchange Format [4], which will be released under a free licence by SupplyScape Corporation and was developed with input from the members of the Drug Security Network. In terms of data content, it will provide not only a superset of what is required by law in various States of the USA, 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

3. Pedigree, Mass-Serialization and Data Sharing / Security

3.1. Pedigree

The purpose of a pedigree is to provide legal proof of a secure chain of custody from the originator of the part through to the organization that receives the part. Two key issues need to be considered:

- Pedigree Data Content/Format
- Pedigree Transmission Mechanism

Published February 1, 2006. Distribution restricted to Sponsors until August 1, 2006

3.1.1. 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 global 'highest common multiple' pedigree format emerges, with the complete superset of traceability information required by the laws of all countries.

- 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 CAGE code, have one field for supplier ID and another field for supplier ID type, such that in the USA, the supplier ID type may be set to 'CAGE' – but may be set to other values in other regions of the world which fall outside the scope of the USA / NATO.

- 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.

3.1.2. 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 parts shipped downstream.

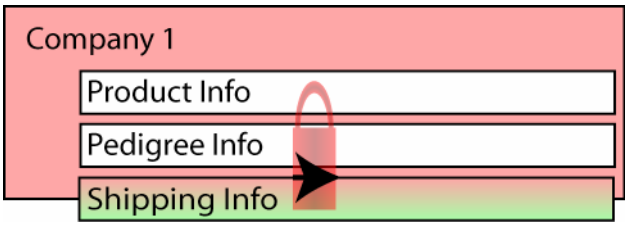
- Suitability for legal/government audit
  - This may have an impact on the decision about how closely to integrate the pedigree into more general-purpose software, such as legacy EDI applications or the EPC Network components (specifically EPC Information Services), since doing so may result in these 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.

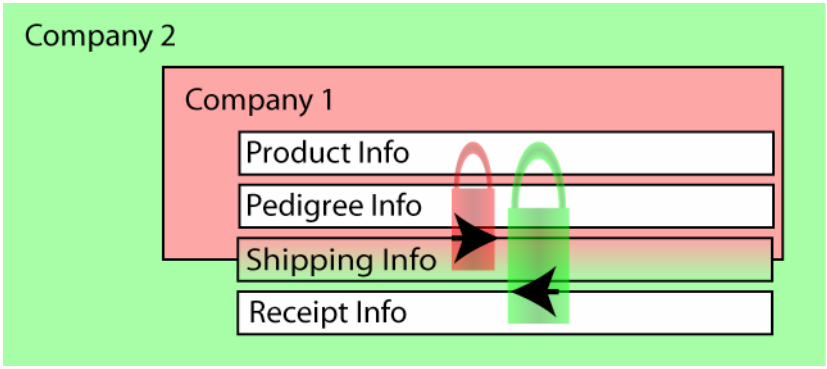
3.1.2.1. Propagating document approach

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 part.

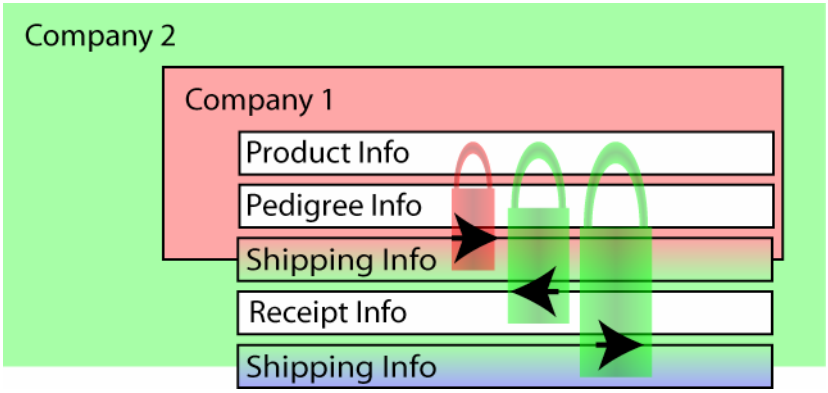
a)



b)



c)



d)

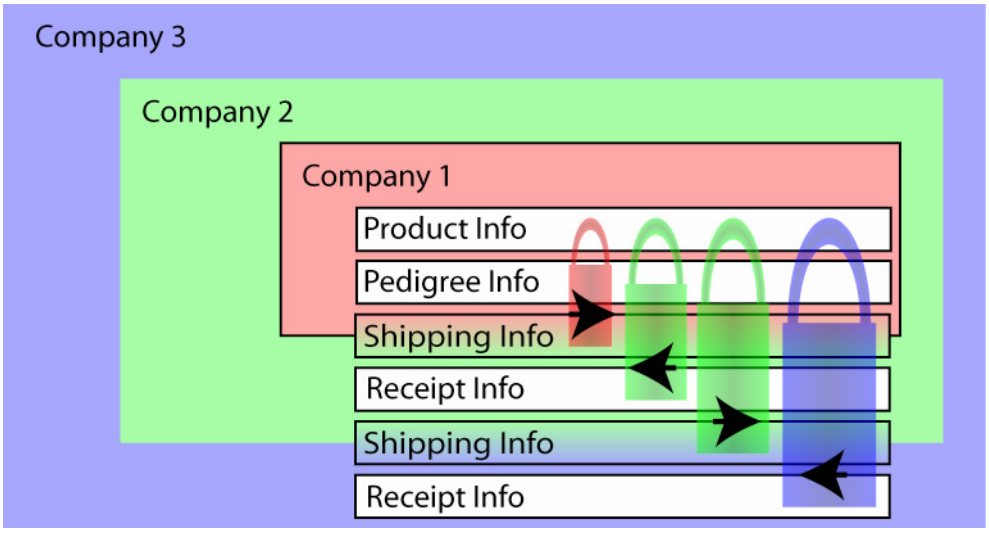


Figure 4 – Propagating document transmission mechanism for pedigree. The padlocks represent a digital signature over the content indicated, effectively providing a tamper-evident lock against over-writing of the information over which the signature applies. Note that by signing both the shipping and 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).

A further major security benefit of the propagating document approach is that as soon as the parts 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 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 other formats. The methodology of constructing digital signatures over parts of XML documents is already standardized by W3C [5], and this is a potential technology solution for such signatures over the transaction data.

3.1.2.2. 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 5.

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.

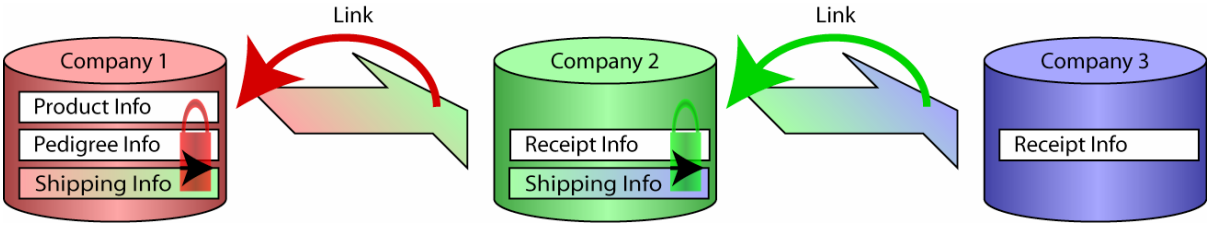
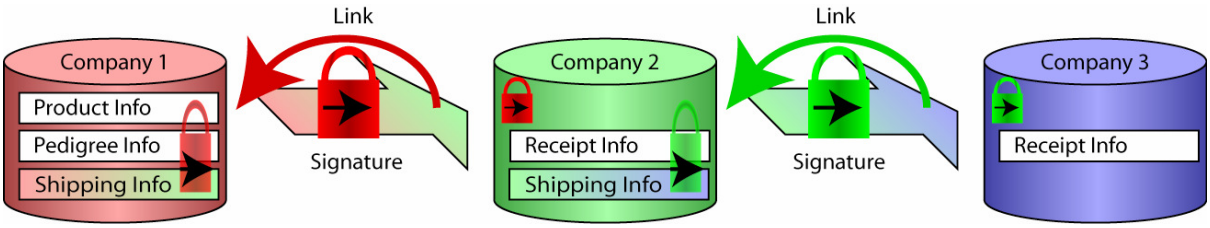


Figure 5 – A simple fragmented data approach to linking of pedigree data. Each company sends the next custodian a link to the pedigree data they hold for the part but retain the data themselves rather than embedding into a pedigree document.

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.

The major vulnerability in this approach is that potentially each company retains the only authoritative copy of their data – and would be in a position to either delete or amend and re-sign modified data, if the company were under investigation. A potential solution 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 6a) and/or to a central registry (see Figure 6b), to which they are granted only one-time write access for each individual package.

a)



b)

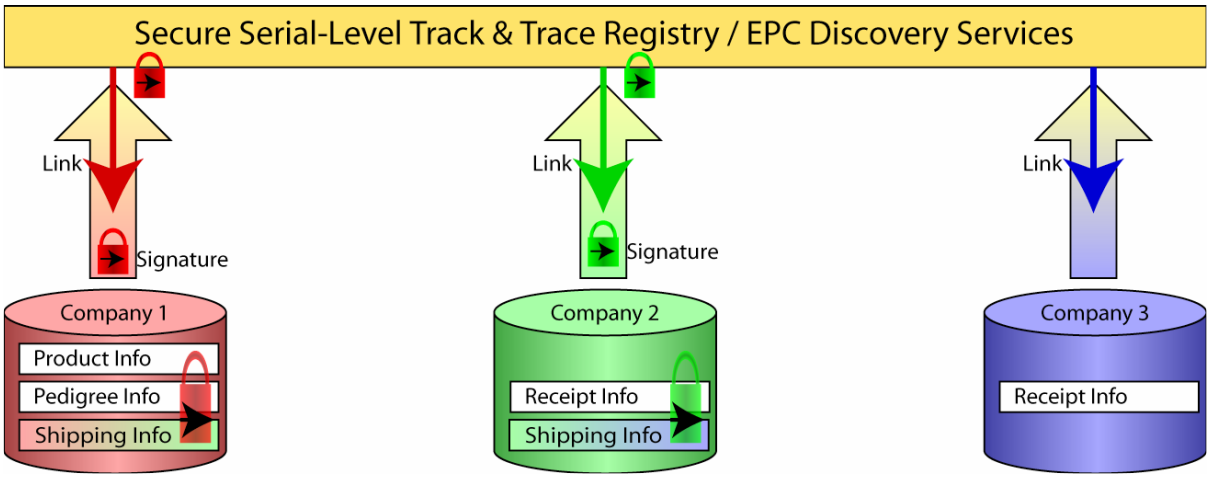


Figure 6 – A more robust mechanism for linking distributed pedigree information.
In (a), the link to the pedigree information is sent from the shipper to receiver and is accompanied by a digital signature, which is retained by the receiver.
In (b), the link to the pedigree information is sent to a secure 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 6a, 6b.

Figure 6b 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. These issues are discussed further in Section 5.3.1.

3.2. Serialization

3.2.1. Requirements

The requirements of an ID number include that it should be:

1. Unique
2. Large enough
3. Extensible
4. Readable via Auto-ID technologies including RFID and barcodes
5. Private
6. Secure
7. Neutral
8. Persistent
9. Global
10. Able to filter on different levels of logistical units (item, case, pallet)
11. Able to support handling of parts at class level (i.e. indicate part type)
12. Easy to administer

A number of additional requirements might be considered:

1. The ID number uniquely identifies an individual part but might not necessarily identify the part type.
2. The ID number points to data on a network and we should refrain from embedding information in the ID itself – although additional information about the part might be stored in the memory of an RFID tag or other device, e.g. memory button.
3. The lookup based on the ID number must be manageable and scaleable to sufficiently large volumes.
4. It may be desirable to check the validity of a genuine ID number by some means (algorithmic – e.g. checksum type calculations – or via a network lookup).

In some countries, the law forbids government agencies (such as the US Department of Defense) from imposing requirements that would necessitate companies complying with those requirements to pay a fee – e.g. to a name issuing authority, in order to comply with the requirements. An example of this is in the Passive Tag RFID guidelines [6] issued by the US DOD as requirements to be included in new contracts with suppliers; although the guidelines embrace the GS1 system, they also cater for non-subscribers of GS1/EPCglobal by specifying how the CAGE and DODAAC codes may be used to encode RFID tags. ATA Spec 2000 currently supports the use of CAGE, GS1 or Dun & Bradstreet DUNS numbers for identifying the manufacturer of a part.

This report does not make any explicit recommendation on how existing unique identifiers in use in the aerospace industry should be represented in Electronic Product Code (EPC) format, other than to note that the EPC is primarily expressed as a Uniform Resource Name (URN) and that there is a close structural similarity between the current US DOD Passive Tag Data Recommendations (appearing in EPCglobal Tag Data Standards as USDOD-64 and USDOD-96) and the ATA Spec2000 unique identifiers for new parts (consisting of

manufacturer and serial number MFR/SER or CAG/SER, DUN/SER, EUC/SER variations where CAGE, DUNS or GS1 identifiers indicate the manufacturer) or in-service parts (consisting of supplier and serial number SPL/UCN or CAG/UCN, DUN/UCN, EUC/UCN variations where CAGE, DUNS or GS1 identifiers indicate the supplier).

3.3. Data Sharing and Security

This section summarizes a number of issues mentioned in the DSN paper [2] 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).

His 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 UML activity diagrams, together with tables of descriptions. Functional acknowledgements, transactions, timeouts and retries are also considered.

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

3.3.1. Use Cases

Three groups of use cases were considered:

- Base Case
  - sufficient to comply with pedigree laws for pharmaceuticals in Florida
  - implemented in practical demonstration (DSN Lab)
- Safe and Secure
  - goes further, contains use cases useful in realizing the vision of a safer, more secure 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 part'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 parts supplier/distributor/parts receiver), triggers, frequency and extensions, issues and notes.

It may be the case that there will be different impacts of electronic pedigree on parts receivers and distributors / suppliers. Distributors may receive goods from their parts suppliers and be required to verify the pedigree, then authenticate and certify the pedigree document, before shipping. A receiver of parts, on the other hand, may only be required to receive and verify, but not authenticate and certify the pedigree document, or to 'close' the pedigree document, especially if the part may be re-used multiple times and have multiple lifecycles. However, when parts have reached the end of their useful life, then consideration should be given to closing the pedigree document and also closing the identifier record, to indicate that the part is no longer fit for further circulation. These ideas are illustrated in Figure 2 of this overview report.

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

1. It will no longer be sufficient to check bulk quantities and part types against a purchase order.
2. 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 parts

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

The paper by Dr. Inaba considers the message choreography in terms of the following:

1. Offer documents (e.g. Purchase Orders (PO), Shipping Notices)
2. Acceptance document (response to offer – need not be electronic)
3. Functional acknowledgement (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 as 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 – 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.

3.3.2. Security

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

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

2. Authorization
   – does the other partner have appropriate authorization to send a business document / deal?
3. Confidentiality
   – is the communication channel private? (e.g. encrypted documents / channel)
4. Integrity
   – is it certain that the business document is not garbled or has not been tampered with?
5. 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.

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

Table 1 – EDI and internet technologies and the corresponding security features they offer

3.3.3. 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 parts 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:

1. Information which is unique to a particular pedigree document (ID, version of format, timestamp)
2. Information which is unique to an individual part (part name, manufacturer/distributor, object ID, NDC, manufacturer date, expiry date, container size, lot number, parent package part ID)

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

3. Information about the shipper
    a. Transaction data (sales invoice number, date of purchase, quantity by lot number)
    b. 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 parts with the pedigree document (verification) then signs the pedigree to confirm receipt (certification). At this point, the parts can be used or put away until needed.

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

4. Information about the shipper
    a. Transaction data (sales invoice no, date of purchase, quantity by lot number)
    b. 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 part.

These processing stages are also shown schematically in Figure 2 of this report.

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

Published February 1, 2006. Distribution restricted to Sponsors until August 1, 2006

3.3.4. File size, bandwidth requirements and timing issues.

Assuming an XML format of the pedigree document and an encapsulation mechanism, whereby the 'inherited' pedigree from previous custodians is encapsulated within a new outer wrapper containing additional information added and signed by the current custodian, the paper considers how the file size of pedigree document grows as it passes from one custodian to the next. It is assumed that the Pedigree Business Document envelope adds a 20% overhead to the total of the file sizes of the component individual pedigrees within the Pedigree Business Document.

The paper then provides an analysis of bandwidth requirements and loading (utilization rate) by the pedigree application, as well as a calculation of number of files in the queue and the waiting times, using queuing theory. The analysis of bandwidth requirements focuses primarily on file transfer times at various bandwidths / bit rates – but also mentions that consideration must be given to the additional time to digitally sign pedigree documents, compress files, etc. Furthermore, the paper notes that the impact of delays on timing choreography and business processes may require the supplier to have a large staging area for shipments awaiting an authentication result document to be returned from the buyers.

3.3.5. 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 ID of each of the parts. 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 parts). 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/transfer

There will be a need to not only design new documents such as the pedigree document and the 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.

3.3.6. Risks of paper pedigree

Appendix G of the paper 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 in the pharmaceutical sector, it carries the following risks:

- Lack of digital signature technology. As discussed in section 4 of this report, 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 complement the paper-based pedigree document.

- Retailers cannot check the authenticity (trade/exchange history) of a part before it is shipped from wholesalers. Wholesalers may not execute granular status control without confirmation messages from retailers.

- Retailers can only verify received products by counting the number of parts and the number of paper-based pedigree documents. Human-readable object identifiers on the parts 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 a pedigree document is printed out rather than being handled electronically, the pedigree (and the associated part) is not transferable (or has a potential risk of counterfeiting). This may also impact the legitimate returns process.

- Receivers of parts do not terminate the object identifiers and associated pedigree documents when the parts are scrapped. Even if they can terminate the pedigree, paper-based pedigree documents may be illegally reused assuming that some parties just count the number of both parts and papers without checking the individual part identifiers.

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

- Distributors can print out paper-based pedigree documents of parts transferred with electronic pedigree – or transferred to other parties with paper-based pedigree documents. Distributors can have more paper-based pedigree documents than

authorized parts. Then, a fraudulent distributor can supply unauthorized parts with legitimate paper-based pedigree documents.

- Receivers of parts can sell paper-based Pedigree documents back to distrbutors. Receivers may be able to sell the object identifiers with paper-based pedigree documents to a distributor. A fraudulent distributor may forge paper-based pedigree documents and supply unauthorized parts saying they are returns from an organization which received them previously.

In summary, using paper-based pedigree documents increases the risks of entry of unauthorized parts. One of the major issues here is that those who receive paper-based pedigree documents cannot validate the trade history of the parts, which is a purpose of implementing electronic pedigree application. This also means that once a pedigree document is printed out, the part should be transferred to a controlled area. If it is allowed to re-convert a paper-based pedigree document into electronic pedigree document, the next receiver should be notified of the risk associated with the parts. The paper also considers conversion between different transport protocols, and the need to ensure that 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?

4. Vulnerabilities

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

4.1 Pedigrees initiated by the distributor/supplier rather than the part manufacturer

In addition to the potential risks associated with paper pedigrees, there is the need for some clarification about how in-service parts 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 a subassembly for each of the smaller parts disassembled 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 subassembly from which parts originated. Ideally, a new pedigree document should be created for a new part ID, which includes and extends the pedigree of the subassembly from which it was obtained. The new part ID may also be used for lookup purposes to find authoritative information services about the part. There may be a legal issue about whether the distributor or the original manufacturer is the authority for that part

Published February 1, 2006. Distribution restricted to Sponsors until August 1, 2006

and accepts the liability that accompanies this role. Finally, if it is allowed to use the original manufacturer's code for the new part 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 part 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 part ID (in this example, the manufacturer) would also be responsible for keeping track of when the part ID is ultimately decommissioned or 'closed', e.g. on scrapping or invalidation.

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

At the point of disposal or scrapping, when the part reaches the end of its life, 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 unauthorized parts 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 supply chain, since this may be an indication of a party attempting to reuse serialized IDs read from scrapped parts to introduce unauthorized parts. Within the architecture of the EPC Network [7], appropriate places to record 'closure' or 'termination' of an individual serialized ID are either in the EPC Information Service provided by the part manufacturer or distributor – or as a 'flag' or field in the appropriate 'EPC Discovery Service' for the records for that individual serialized part ID.

4.3. 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.

The only permissible conversion between paper and electronic formats is as follows:

1. An entirely electronic pedigree document is printed out or faxed onto paper.
2. The recipient scans the document and performs optical character recognition (OCR) to regenerate the text file that was originally sent.
3. The text file should be canonicalized, to ensure that no additional white spaces or line break characters have been inadvertently introduced.
4. 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.
5. 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.

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.

4.4. 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 parts, the public/private key may be 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 safety of aerospace parts, e.g. US Federal Aviation Administration. 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.

4.5. Enforcing a change of serial ID and labeller code on changes of part aggregation

When a subassembly is broken down into individual parts, it is essential that new serial IDs are created for each of the resulting parts, so that each is independently traceable for pedigree purposes. The new serial IDs should reflect the ID of the distributor, rather than the

ID code of the original manufacturer of the subassembly 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 parts can be correctly resolved to the appropriate information records.

5. Next steps and outstanding issues

5.1. Pedigree – Next steps

Documentation on the Open Universal Electronic Pedigree Interchange Format is available for download without charge from http://www.epedigree.org, subject to the terms and conditions of the licence agreement. EPCglobal has announced a process to begin standardization of the pedigree format for the pharmaceutical sector and a work group to investigate closer integration with their EPC Information Service interface for access to pedigree information. A number of other technology solution providers have already announced their willingness to contribute their pedigree schema as input into the work group – and according to the declaration on the website http://www.epedigree.org, SupplyScape Corporation are also intending to contribute the Open Universal Electronic Pedigree Interchange Format to the EPCglobal work group when it is formed. Aspects of the pedigree standard developed for the pharmaceutical sector at item level may also be relevant for item-level aerospace parts.

5.2. Serialization – Next steps

ATA Spec 2000 currently uses ASCII text representations of the identifiers using Text Element Identifiers (TEIs) (usually 3-letter codes such as MFR, SER, etc.) to distinguish between the manufacturer/supplier field and the unique serial number.

Electronic Product Codes (EPCs) are usually expressed as Uniform Resource Names (URNs) where a dot character separates the company ID (MFR or SPL in the context of Spec 2000) from the serial number (SER or UCN) and rather than literally encoding TEI codes within each identifier, the hierarchical structure of a particular URN is understood to contain particular data fields arranged in a particular order (e.g. MFR followed by SER).

For RFID tags with sufficient memory capacity, there is generally no problem in encoding such identifiers as one byte of data per ASCII character. For low-cost passive tags, as used by the consumer retail sector, memory capacities are much lower – typically of order 96 bits. In this case, some elements of the EPC in URN format are compressed or compacted when encoded into binary. For example, in the consumer retail sector, the EPC URN prefix ‘urn:epc:id:sgtin:’ is compacted to a single 8-bit header, [actual value 30_{hex} ($48_{decimal/ASCII}$)] for use on a 96-bit tag, i.e. the prefix occupies 1 byte rather than 17 bytes. Likewise, the US DOD use 6-bit compaction of each byte for use in 64-bit tags for their coding schemes.

Published February 1, 2006. Distribution restricted to Sponsors until August 1, 2006

Even if tags with larger memory capacity are routinely used with aerospace parts, it may still be very worthwhile for the aerospace industry to align their unique identifiers with a format that is compatible with the EPC identifier format, so that commoditized equipment and software conforming to EPCglobal standards can be used at least for reading the unique identifier from each part.

ATA Spec 2000 already defines a number of unique identifiers which are suitable for part tracking – and generally consist of a manufacturer (MFR) / supplier (SPL) code and a unique serial number (SER or UCN). A number of name issuing authorities are supported, including US DOD/NATO (CAGE code), GS1 (formerly EAN.UCC) and Dun & Bradstreet.

There is already a precedent for delegation to agencies other than GS1 as name issuing authorities, as in the case of the US Department of Defense. Under new contracts issued by the US DoD, suppliers are required to begin tagging products using passive RFID tags. While they advise their suppliers who are also subscribers of EPCglobal to use the SGTIN and SSCC formats of EPC, they needed to provide a mechanism for non-subscribers of EPCglobal to uniquely identify supplies shipped to the US DoD – and for this, US law does not permit any government agency to require a fee for the privilege of doing business with it. This was resolved by allocation of two EPCglobal header codes to the US DoD (who are a subscriber of EPCglobal), in order to support their serialization structures based on the CAGE and DODAAC codes. For non-subscribers of EPCglobal who supply to the US DoD, the US DoD (or NATO for non-US suppliers) act as a name issuing authority and allocate CAGE and DODAAC codes to suppliers.

It would be helpful to receive clarification from the US Federal Aviation Administration (US FAA) if they consider that as a government agency, they are bound by the same legal restriction, i.e. at some time they may require mass serialization to be mandatory – but may need to provide a mechanism for compliance which does not require payment of a fee to any organization.

The appropriate technical forum within EPCglobal for standardizing the serialization format for aerospace parts is the Tag Data Standards work group within EPCglobal's Software Action Group. The EPC representations of the US DOD formats have already been defined in the ratified Tag Data Standards document [8] v1.1 revision 1.27, published on EPCglobal's website.

When the serialization schemes are formally included in a future revision of EPCglobal's Tag Data Standards, the final step is to prepare an XML definition file for EPCglobal's Tag Data Translation standard (to be ratified January 2006). This will greatly ease the process of mapping between the serialized identifiers, legacy formats (labeller codes and serial numbers) and binary formats to be stored on the RFID tags.

5.3. Lookup services

5.3.1. Object Name Service and Discovery Services

Mass-serialized unique identifiers are essential for ensuring that there is an inviolable one-to-one association between an individual part and its pedigree record. They are also very useful for accessing serial-level information specific to each individual part. This might include serial-level master data held by the manufacturer as well as additional transaction data and other lifecycle data held across the entire supply chain – and in the case of aerospace parts, information held for multiple lifecycles of that part. The unique identifier acts as a licence-plate for the package, allowing additional information to be retrieved from networked databases. This is the design philosophy behind the Electronic Product Code (EPC) Network [9][10] designed by the Auto-ID Center [11] and now being commercialized and standardized by EPCglobal.

Many organizations may hold some data about an individual part, although usually only one organization holds the definitive or authoritative information, such as the date and place of manufacture. Within the EPC Network Architecture [7], there are two kinds of lookup services – the Object Name Service (ONS) [12], which points to authoritative sources of information for a particular EPC and EPC Discovery Services, which point to multiple additional sources of information, at serial-level resolution, right across the supply chain.

The Object Name Service (ONS) is built using DNS technology and provides only pointers to authoritative information. Figure 7 shows the hierarchical organization of the Object Name Service, ONS.

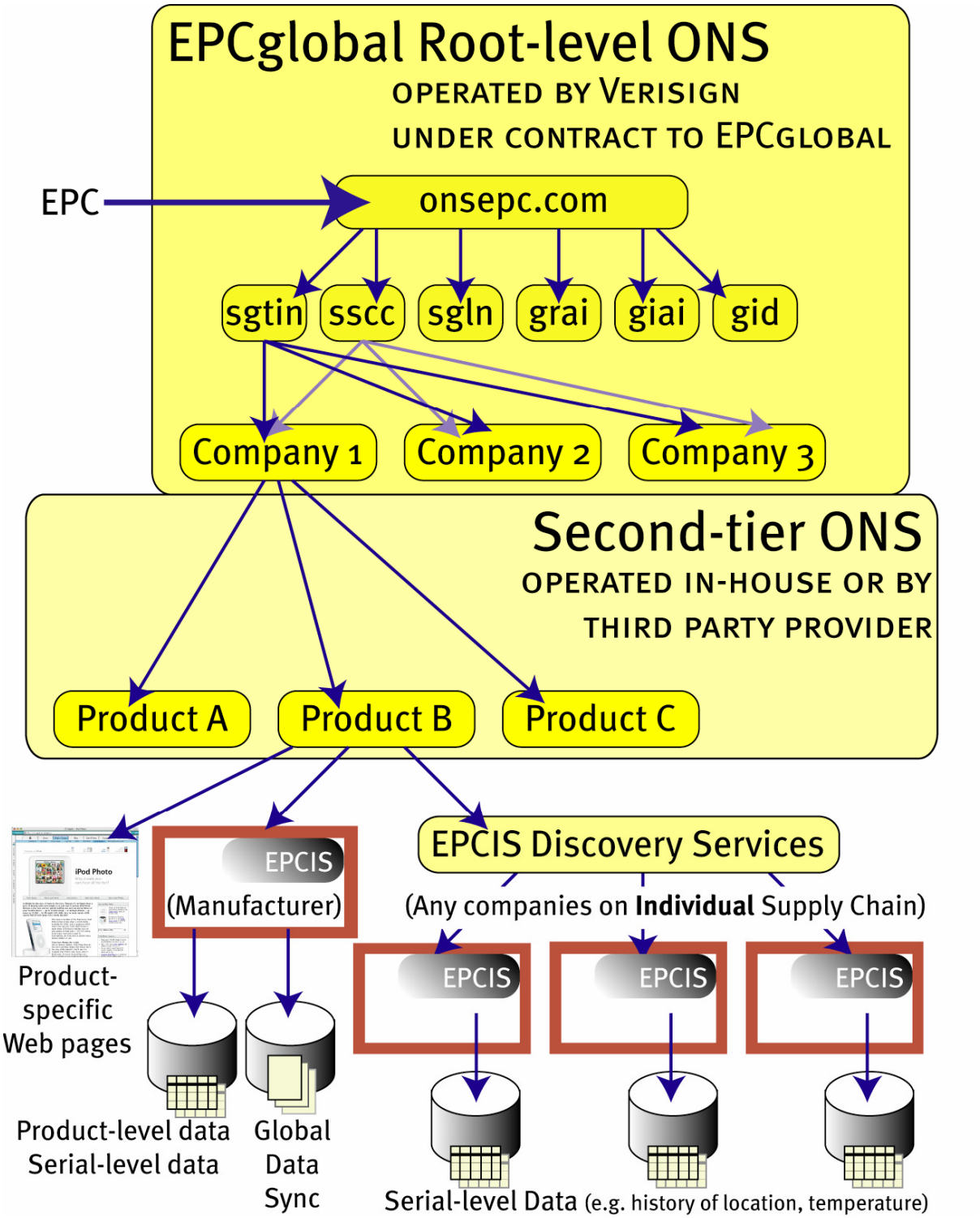


Figure 7 – Hierarchical organization of the Object Name Service (ONS).

The root-level ONS (operated by Verisign under contract to EPCglobal) resolves the Company Identifier. A second-tier ONS can resolve different categories within a company.

The second-tier ONS is simply a DNS configuration that can be implemented in-house or provided by any competent technology solution provider.

In the case of the SGTIN EPC used in the FMCG sector, ONS records typically resolve the product type, but not the serial number, because it is feared that to do so might harm the DNS system which powers the internet, because of the high volumes of consumer goods in circulation. EPCglobal have not yet defined whether ONS will provide serial-level pointers for other coding schemes such as SSCC [13] etc. – or whether an alternative mechanism, such as Discovery Services (see below) will be used in tandem with ONS.

There are potentially multiple providers of serial-level information across the entire supply chain followed by an individual object, since each party may have collected and recorded some information about it. The EPCglobal Network Architecture document anticipates the need to provide for serial-level track and trace across the supply chain and 'Discovery Services' are intended to fulfil this role. To date, EPCglobal have not yet chartered a work group to begin standardization of the interface for Discovery Services, even though there has been some discussion on this issue within EPCglobal's Architecture Review Committee.

Having said that, there are a number of technology vendors who are already providing solutions which they call 'Discovery Services', although it must be understood that there is not yet a ratified EPCglobal standard interface guaranteeing interoperability between the different Discovery Services from different technology vendors, nor has a work group even been chartered to begin standardization of this important element.

There are justifiable concerns from government regulators about which organizations would provide such Discovery Services and what the business model may be. Anti-trust law, pro-competition or anti-monopoly laws clearly need to be considered in each jurisdiction. Many government agencies may find that by law, they cannot introduce legislation which requires manufacturers or suppliers of parts to pay a fee or subscription to a non-governmental agency, whether a technology provider or even a not-for-profit organization such as EPCglobal. It may therefore be the case that an appropriate government agency administers such a Discovery Service on behalf of the aerospace sector within their geographic jurisdiction and requires all aerospace supply chain parties to provide the relevant data updates for track and trace purposes, with no direct fee or subscription payable by the supply chain companies. The cost of operating the Discovery Services would then be borne by the government agency and paid out of general taxation and/or revenue from registration fees that some agencies might charge to authorized part suppliers within their territory. If the government agency is not confident that it has the in-house expertise to implement Discovery Services, it can of course sub-contract the installation and day-to-day operations to one or more technology solutions providers, after an appropriate tendering process and checks of due diligence on data security, robustness, etc.

A further issue concerning Discovery Services is the global nature of supply chains themselves. Would a government agency such as the US FAA have the authority to require updates to be sent by supply chain parties outside of US territory? Is it even desirable to have separate Discovery Services for the aerospace sector in USA, Canada, Europe, Middle East, Asia, Africa, South America or Australasia especially given the global nature of the aerospace business? If multiple regional Discovery Services were installed and the mass-serialization scheme adopted only identified a Manager ID and a long serial number, how

could a record in the EPCglobal Object Name Service point to the appropriate Discovery Service for that particular serial number?

[In fact, the EPCglobal Object Name Service (ONS) provides a partial solution provided that if is possible for each labeller to include some structure to the serial number, (e.g. leading digit=1-2 → USA, 3-4 → Europe, etc.) and to be able to designate this regional coding at the time when the unique identifier is attached to the part. In this case, the records in ONS could make full use of the regular expression pattern matches for the NAPTR records. In simple terms, this means that for each supplier of parts, there would need to be an ONS entry for each of the world's regional Discovery Services, where the pattern to match is not simply 'match all' – but is specific to some structured element present in the serial number. The ONS lookup is then slightly more complicated, since it involves checking the serial ID or EPC in pure-identity URN format against the patterns from the ONS records and picking the matching entry to obtain the address or URL of the appropriate regional Discovery Service for that specific serial number.]

5.3.2. Impact of Serialization Choices

5.3.2.1 Lookup via EPCglobal's Object Name Service (ONS)

If EPCglobal were to decide not to allocate an EPC header to the serialization scheme proposed by the aerospace industry, then allocation of an ISO AFI header may be an alternative option for the aerospace industry to consider, although it must be borne in mind that the identifiers would then be outside the EPCglobal Network, may not use the 'urn:epc:' prefix nor would the EPCglobal root Object Name Service (ONS) provide resolution of these identifiers. Alternative resolution mechanisms would need to be implemented. However, it is technically feasible to set up an alternative root-level Object Name Service, since the Object Name Service (ONS) is simply an implementation of the Domain Name System (DNS) and the ONS standard is now ratified and therefore available for download from the website of EPCglobal.

5.3.2.2. Next steps – co-ordination across the supply chain

In terms of the database servers themselves, a standardized interface for query and capture of data is essential for smooth interaction between trading partners. The EPC Information Service (EPCIS) work group within EPCglobal's Software Action Group is making good progress on a draft specification, which will standardize the interface, particularly for serial-level data, not only providing access to low-level captured RFID read events, but also EPC-related data with higher-level contextual information, such as associations with business transactions, business process steps and associations between objects (e.g. parent-child relationships). Members of the aerospace industry are recommended to become more

involved in this work, to ensure that the requirements of the aerospacce industry are being fully considered.

The role of the serialized identifier is two-fold – to uniquely identify each object – and to serve as a lookup key for accessing serial-level data in networked databases. In many situations, it will be the original part manufacturer who has authoritative data about the part, both in terms of class-level product master data (e.g. material composition etc.) and serial-level instance data (e.g. date of manufacture, lot number etc.). In other situations, a distributor or parts supplier may maintain the authoritative data. This impacts on the resolution mechanism or lookup service, especially if ONS is used.

Although the topic of what are now termed 'Discovery Services' has been discussed occasionally between members of the EPC-IS and ONS work groups within EPCglobal's Software Action Group, EPCglobal has not yet formally chartered a new technical work group within the Software Action Group to standardize the interface for Discovery Services. The aerospace industry may have a more urgent need for this than the FMCG sector, particularly if they reach large-scale item-level tagging before it is widespread throughout FMCG. If so, then the aerospace industry needs to begin to define its requirements for Discovery Services and consider requesting that EPCglobal charter a work group to begin standards development on this missing component of the architecture.

5.4. Information services – authentication of the product and identity

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 1. A networked information system, such as one complying with the future EPCIS standard, would provide a mechanism for a parts manufacturer or supplier (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. Explicitly 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:

> '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 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 indicates successful authentication. The aerospace industry needs to consider whether this type of query approach is sufficient for object authentication purposes or whether other types of query are needed in the EPCIS standard.

6. Recommendations for future work

6.1. Research and Development work

In order to analyse the operation of the controlled aerospace parts supply network a comprehensive model needs to be developed. This model should be able to be used from any of three perspectives, part centric, actor centric or aircraft centric. This will enable considerations of pedigree data storage on parts, authentication issues by actors and configuration control needs of aircraft all to be considered.

As adoption of mass-serialization and RFID deployment extends beyond relatively limited point-to-point trials to full-scale deployment involving most participants, there will be a greater need for lookup mechanisms that can indicate all relevant sources of information for an individual serialized package. This is necessary in order to be able to gather complete lifecycle history of the part. Such information may be critical to determining the effective remaining usable life of the parts.

There is a need for further research into highly scaleable lookup mechanisms, such as distributed hash tables and overlay networks which were originally developed for peer-to-peer file-sharing networks but may also be relevant for navigation through potentially billions of parts in circulation.

Further research and development on encryption and access-control mechanisms for RFID tags is required, particularly to provide fine-grained security of various elements of (potentially confidential) information which might be stored on the tag in addition to the unique identifier.

Further research is needed in cryptographic or algorithmic validation of serial numbers against products, to try to reduce the need for a network / database lookup each time. At the simplest level, the identifier may incorporate a checksum component and be accompanied by a digital signature of the identifier, signed by the issuer (e.g. manufacturer). This is particularly important for backup purposes, to enable authentication of the product, even when access to the internet or the manufacturer's networked databases is not available.

6.2. Standards Development

Standards bodies such as EPCglobal and others need to consider chartering a new work group to begin specifying a standard application programming interface or API to Discovery Services. This interface will need to have at least the same levels of security as for the EPC Information Services and should support at minimum basic tracking and trace functions (updating and queries), although the access control policies implemented may restrict who is allowed access to these functions. Additional features might include the ability to record closure of an ID – or its current state, as well as meta-data to describe the role of each custodian handover event or transaction. To deal with the repackaging issue, it might also be advisable for Discovery Services to be able to maintain a link from an old ID (e.g. of a subassembly) to (multiple) new IDs of parts obtained from its disassembly.

Standards bodies should be working closely with regulatory bodies (both governmental and industry associations) around the world to publish a standardized comprehensive pedigree format and to agree appropriate standards on accompanying business documents and messages. The paper by Dr. Inaba may provide some useful guidance which is also relevant to the aerospace sector.

6.3. Opportunities for technology solution providers

There are clearly opportunities for pedigree management applications, to facilitate reconciliation of pedigree IDs with part IDs, purchases orders, invoices, advance shipping notices and advance pedigree notices. Such tools should also be able to verify all the digital signatures of previous custodians.

There are also opportunities for the development of data mining applications which access Discovery Services and EPC Information Services and automate the detection of suspicious behaviour (e.g. the same part ID appearing simultaneously in multiple distant locations), diversion activities etc., enabling better use of human operator time to make an informed judgement about possible suspicious behaviour, rather than spending time merely gathering the information.

6.4. Actions for regulatory bodies

Regulatory bodies in all countries should work together to achieve global convergence on comprehensive harmonized requirements for:

- pedigree information.
- mass-serialized identifiers for aerospace parts.
- business processes required to achieve a safe and secure supply chain.

Regulatory bodies need to work with the relevant standards organizations to formalize the appropriate global standards.

Regulatory bodies also need to be very clear in their statements of requirements, to ensure that there is no ambiguity about the following topics:

- How to implement mass-serialization in a way that protects supply chain security.
- Security and retention of pedigree-related data – and penalties for failing to provide this data upon demand within a specified time to authorized inspectors.

References

[1] 'Serialization Options for Tracking of Pharmaceuticals using Radio-Frequency Identification', M. G. Harrison, 2005 – DSN White Paper #1.

[2] 'Technical Issues of Electronic Pedigree Inter-organizational Transactions', T. Inaba, 2005 – DSN White Paper #2.

[3] 'The Drug Security Network – An Overview and Discussion of Remaining Issues', M. G. Harrison, 2005 – DSN White Paper #3.

[4] 'Open Universal Electronic Pedigree Interchange Format', http://www.epedigree.org

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

[6] US DOD Suppliers' Passive Information Guide
http://www.acq.osd.mil/log/rfid/supplierguide.htm

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

[8] 'EPC Tag Data Standard' v1.1 rev. 1.27
http://www.epcglobalinc.org – see under 'Standards and Specifications'.

[9] "The Networked Physical World - Proposals for Engineering The Next Generation of Computing, Commerce & Automatic Identification"
Sanjay Sarma, David L. Brock, Kevin Ashton (2000)
http://www.autoidlabs.org/whitepapers/mit-autoid-wh-001.pdf

[10] EPC – Electronic Product Code
"The Electronic Product Code (EPC) - A Naming Scheme For Physical Objects",
David L. Brock (2001)
http://www.autoidlabs.org/whitepapers/mit-autoid-wh-002.pdf

[11] In October 2003, the Auto-ID Center transitioned into two organizations:
1) Auto-ID Labs [http://www.autoidlabs.org] continue the research activities
2) EPCglobal Inc. [http://www.epcglobalinc.org] manage the standards development processes and commercial adoption of the EPC Network.

[12] Object Name Service (ONS) standard v1.0
http://www.epcglobalinc.org – see under 'Standards and Specifications'.

[13] SSCC – Serial Shipping Container Code
http://www.uc-council.org/ean_ucc_system/pdf/SSCC.pdf

Published February 1, 2006. Distribution restricted to Sponsors until August 1, 2006

Appendix 1 – 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 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.

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.

After an initial plenary kick-off meeting, 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. A 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 the DSN was to undertake focussed brainstorming among major players in the pharmaceutical sector, 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 and standards development processes at EPCglobal and elsewhere.

The primary deliverables of the DSN activities consist of three papers:
The first paper [1] is entitled ‘Serialization Options for Tracking of Pharmaceuticals using Radio-Frequency Identification’, authored by Dr. Mark Harrison of Auto-ID Labs at Cambridge, UK. This is summarized in Section 3.2 of this report.
A second paper [2] 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 Section 3.3 of this report.
The third paper [3] provides 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 that still need to be addressed.

Appendix 2 – Authenticating the part

When validating the authenticity of the part, 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 supplier applied to the part?

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 supplier?

Authenticity of the serialized identifier

- Is the serialized identifier programmed into the tag a valid one?
- Has that particular serialized identifier been issued by the manufacturer or supplier?
- 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 parts or all serial numbers within a part type)?
- Do the information services have a record of the security features to expect (and where to find them) – and those not to expect?
- 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 still available for distribution and use or has it already been decommissioned / de-authorized / invalidated, etc.
- Is the information record corresponding to that serialized identifier now closed?
- Is the serialized object still in circulation beyond the date when the part was scrapped?

Authenticating the trail

- Can the pedigree trail be verified for all previous custodians?
- Has the part 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?)

Appendix 3 – Glossary

Term	Definition
CAGE code	A *CAGE Code* is a five-position code that identifies contractors doing business with the Federal Government, NATO member nations, and other foreign governments. It stands for *Commercial and Government Entity.*
Canonicalization	In information technology, canonicalization is the process of making something canonical - that is, in conformance with some specification. To canonicalize is to ensure that data conforms to canonical rules, and is in an approved format.
DODAAC code	This is a code that identifies an entity in the US Department of Defense supply network. DODAAC stands for *Department of Defense Activity Address Code*.
DUNS number	Dun and Bradstreet maintain the *DUNS* company identifier system utilized by both government and corporate officials searching for background information on companies. DUNS stands for *Data Universal Numbering System.*
GS1	GS1 is a leading global organisation dedicated to the design and implementation of global standards and solutions to improve the efficiency and visibility of supply and demand chains globally and across sectors.