

RFID Tag Data Security Infrastructure: A Common Ground Approach for Pharmaceutical Supply Chain Safety

Joseph Pearson, Business Development Manager
Texas Instruments Radio Frequency Identification Systems

Executive Summary

Raising consumer confidence about the authenticity of its prescription drugs is the end goal for the pharmaceutical industry, especially as the number of counterfeit, gray market and diverted products continues to climb. Radio Frequency Identification (RFID) technology, when combined with a secure tag and data infrastructure, can assure both package authenticity and pedigree while creating new revenue opportunities. And while manufacturers, distributors and retailers continue to expand collaborative RFID pilots, and may agree on their goals, they're not all on the same page when it comes to deployment methods.

For the pharmaceutical industry to create a secure supply chain using RFID technology at the item-level, it needs a broader and more flexible approach – one that encompasses all stakeholder requirements and provides a range of implementation options.

The industry is currently working toward the development of a new Item-Level Tagging (ILT) standard. This paper proposes requirements for ILT deployment and lays the foundation for a Tag Data Security Infrastructure (TDSI) for these initiatives. It defines the key deliverables and outlines the requirements of this “common ground” approach. The TDSI is designed to expand and unify the industry's information technology ecosystem by incorporating both centralized and decentralized deployment options.

Elements Necessary for Deploying RFID at the Item-Level

One of the primary reasons the pharmaceutical industry is exploring RFID technology at the item-level is because it offers external validation of a product's authenticity and provenance. Determining if pharmaceutical products in the supply chain are genuine automatically and without human intervention is simply not economical without RFID. RFID tags applied to products within a secure infrastructure raise the level of confidence that the product is genuine on two fronts: by determining the authenticity of the packaging, and by providing automated traceability to create an itemized electronic pedigree, or record that an item has passed through authorized entities.

While all stakeholders in the pharmaceutical supply chain appreciate the value of these RFID benefits for Item-Level Tagging, there are three essential elements necessary to move the industry from selective pilots to full-scale deployment.

1) Participation by all Segments – Manufacturers, Distributors and Retailers

Pharmaceutical manufacturers do not differentiate themselves from competitors based on new technologies designed to make their supply chains more efficient, nor does the industry possess powerful retailer advocates to mandate adoption. Regulatory guidance, through Congressional legislation overseen by the Food and Drug Administration (FDA), is necessary for industry-wide adoption of RFID by all supply chain participants. Additional motivation, or lack of active resistance, comes from RFID's potential to generate revenue and reduce operating costs. RFID could be used to reduce the amount of chargebacks by making product processing more efficient or eliminating illegitimate chargebacks altogether. "Chargebacks occur when the wholesaler sells a drug product at a contract price lower than what he/she paid. The chargeback is the difference between the manufacturer's price to the wholesaler and the contract price to the customer. The wholesaler will submit a chargeback request to the manufacturer on a regular basis (daily or weekly)."¹ Manufacturers have problems validating whether a chargeback is legitimate or if a single product has already been credited as a chargeback from another wholesaler. According to industry analyst firm IDC, up to 5 percent of some product's potential revenue is reduced by chargebacks. Thus, improvements in this area can be made by associating a chargeback to a specifically tagged product, significantly boosting a manufacturer's net revenue. As pharmaceutical pilots continue to proliferate, the industry will further uncover new revenue-generating and cost-saving opportunities using RFID.

2) Development of an ILT Specification

For RFID to be implemented broadly for pharmaceuticals, common technical and standards-based operating procedures are required. EPCglobal, Inc., through the participation of its pharmaceutical supply chain and technology provider members, is uniquely positioned to guide the development of ILT RFID specifications and methodologies. There are four areas of importance for the development of an ILT specification:

RFID Air Interface Communication – The air interface protocol defines how tags talk to readers. Currently, ISO/IEC 15693 (high-frequency) and EPC Gen 2, Class 1 (ultra-high frequency) are the two internationally-accepted air interface protocol standards being used by the pharmaceutical industry. There are also a few proprietary protocols being implemented in pilots. A single, standard RFID air interface communication is necessary for industry-wide deployment. EPCglobal has active working groups to create ILT specifications with the necessary air interface communication attributes that meet performance requirements. It is anticipated that ILT specifications will be ratified by mid-2007, and they will include faster data rates for reading and programming.

Data Scheme – The data scheme defines the memory structure of the tag, how the numbering will take place, and how the data will be used. Unlike the retail segment, many pharmaceutical manufacturers are reluctant to put product information onto the EPC number scheme due to consumer privacy concerns. Many pharmaceutical pilots have not used the standard EPCglobal data scheme for item-level tags, but have used variations of an EPC number which is void of any product information. In addition to the existing data scheme, the EPCglobal ILT specification will likely include an optional EPC numbering scheme that allows for unique serialization without product information.

Software and Security – Once information is gathered from the tag, a standard approach for associating data with the tag and methods for data transmission will be used. Common middleware software architecture will need to be established to take advantage of the tag data. Also, if tag data needs to be encrypted, a standard cryptographic method will need to be used.

Flexible Implementation – Even with standards-based methodologies, options can be built in that offer flexibility in deployment. For example, users of MS Outlook™ use the same software, but can send and receive emails in plain text or HTML, and the system adapts to user preferences. The ILT standard should allow optional methodologies for all parties and provide reconciliation to accommodate the reality that one size does not fit all.

3) Infrastructure Capabilities

Inherently, a supply chain is comprised of an information technology (IT) infrastructure that employs both centralized and decentralized applications. When RFID tags and readers are deployed within supply chains, they should support both elements.

At the network level, important product information about an item and its status at any point in the supply chain can be made available through networked databases. EPCglobal has established the SGTIN 96-bit numbering scheme with the tag's unique number acting as a network pointer for information about a particular tagged product. For macro supply chain applications, this is sufficient, but centralized network access is not ubiquitous throughout the supply chain.

In the IT world, the common expectation is for on-demand networks with centralized data availability, but this is not the case with the fragmented nature of a supply chain. In many pharmaceutical environments, there is value in information being made available between an RFID tag and reader in a decentralized manner. One example is an RFID smart shelf whose integrated reader constantly polls products to automatically capture inventory. Here it makes sense for the tag on a product to tell the reader what its expiration date is, instead of the reader's host processor connecting to a look-up table stored in a network database.

One of the core requirements for mass adoption of RFID ILT is reconciliation among all supply chain participants on the nature of the IT infrastructure regarding centralized and decentralized sources of data. The TDSI aims to create common ground on the necessary infrastructure for ILT deployment in the pharmaceutical supply chain.

What is a Tag Data Security Infrastructure and Why is it Needed?

The ability to have deployment “options” within a “standard” item-level tagging infrastructure is not an oxymoron. The Tag Data Security Infrastructure (TDSI) is a set of rules, specifications and common

protocols that allow item-level tags and readers to work within and across the industry's information technology ecosystem. First, it always supports network-based applications. Secondly, it bridges the centralized/decentralized infrastructure divide that exists among pharmaceutical sectors by augmenting network-based applications with the capability of anytime, anywhere authentication and product information.

The TDSI addresses the contentious points of whether or not to put product data (e.g. the National Drug Code (NDC)) on the tag; how to authenticate products; ways of ensuring consumer privacy and how to secure tagged products at the case, pallet and item level.

An item-level tagging standard has yet to be defined, so the timing is right for RFID tag, reader and security technology providers to bring a fresh solution to the industry as it debates the specifications, rules, and methods of supply chain collaboration in the EPCglobal standards development process.

Deliverables Supported by the Tag Data Security Infrastructure

As the definition of the TDSI takes shape, there are a series of deliverables it should support. These areas encompass the important concerns of all the various industry stakeholders in the pharmaceutical market, including the Food and Drug Administration (FDA), the Pharmaceutical Research and Manufacturers of America (PhRMA), distributors, retailers and consumers.

Electronic Pedigree (ePedigree)

In June 2006, the FDA decided not to extend the stay or further delay the portion of the Prescription Drug Marketing Act of 1987 that created a legal requirement for pedigree. Previous stays had been issued due to the technical impracticalities of implementation. In early 2004, the FDA suggested that new track and trace technologies like RFID could be used to accomplish and surpass the goals of the PDMA by automatically identifying and tracking the movement of every package of drugs from production to dispensing².

Over the past several years, states, led by Florida, began enacting legislation requiring pedigrees for prescription drugs distributed within their boundaries. These initiatives, combined with the push by the FDA and the newly-established EPCglobal pharmaceutical and healthcare efforts, prompted the industry to take a serious look at the benefits of item-level RFID tracking, beginning in 2005. However, even though many states' ePedigree legislation initially included item-level product tracking, compromises, as in Florida, resulted in final laws requiring only electronic shipping notice verification. One exception is California, which is maintaining its course toward mass serialization at the item level.

Thus, there are two definitions of electronic pedigree today. The first type, a serialized RFID approach (referred to further in this paper as item-ePedigree), gives each product its own specific number which can be automatically captured as the product moves from one point in the supply chain to another. The second, a simple file management approach, does not require product serialization. So while you may know the *number and type* (e.g. 50 bottles of X drug) of products that have been shipped or received, there is no easy way to accurately *verify* the exact products.

Product Authentication

If a pharmaceutical product is authentic, then it is enclosed in the genuine package the manufacturer supplied for it. RFID technology for electronic authentication has numerous advantages: it is more direct and less complex; it can be implemented more expeditiously and expanded easily, and it provides immediate safety benefits where they are most needed, to patients at the dispensing level.

According to PhRMA, “Electronic authentication at the dispensing level provides a direct means of determining in real-time whether a particular packaging unit is authentic (e.g., labeled by the manufacturer). This differs from a pedigree system, which is, ultimately, the recording of a series of authentications at each trade once the package unit has left the manufacturer.”³

PhRMA supports product authentication of pharmaceuticals, stating that, “Critical to this enterprise [the integrity of the American drug supply] is the ability to verify the authenticity and integrity of the original pharmaceutical packaging unit before drug product is dispensed to a patient.”⁴

Product authentication using RFID can be accomplished using a centralized (e.g. checking the product via a central database) or off-network decentralized approach. A decentralized approach allows RFID readers the capability of authenticating the RFID tag on a package via Public-key Infrastructure (PKI) security, which requires cryptographic software in readers and key distribution. Many enterprises protect the security of their communication and business transactions using PKI. By programming PKI digital signatures onto RFID tags, the authenticity of the tag can be ensured. (For more information on PKI, see TI’s white paper “Securing the Pharmaceutical Supply Chain with RFID and Public-key Infrastructure (PKI) Technologies,” at http://www.ti.com/rfid/docs/manuals/whtPapers/wp-RFID_and_PKI.pdf)

Product Information and Privacy

Product information should be associated with the RFID tag, but the debate continues as to whether or not it is needed on the tag itself. Some of the leading manufacturers, distributors and retailers have diverging views on the issue. Several questions should be answered, including:

- If product information resides on the tag, how are consumer privacy concerns addressed?
- How should the product information be associated with the tag, taking into account the varying level of infrastructure investment?

Distributors and pharmacies can realize process efficiencies from a decentralized approach of having product data encrypted on the tag for smart-shelf inventory management, automatic pick and place, and product returns. When it comes to NDC product information, the FDA’s position is that it should be encrypted *or* available via an accessible link. The TDSI can bridge the gap in these two approaches.

Security

The TDSI can provide security at the case, pallet, and item level. Visually-blank labels incorporating RFID placed on cases are being used to deter theft in the supply chain, but with the tag data being broadcast to the readers anywhere from one to 30 feet away, information becomes available to anyone with a handheld reader. By incorporating an encryption option on the tag, product information will not be broadcast, which may prevent the product from being stolen or diverted.

Supply Chain Data Exchange

Automated data exchange is beneficial to the entire pharmaceutical industry. RFID facilitates information exchange automatically at all points in the supply chain, increasing safety and security while improving business processes. Faster and more accurate supply chain data exchange enables item-ePedigree while increasing operational efficiencies in chargebacks and demand forecasting.

Standards-based and Interoperability

The TDSI should incorporate a single-solution approach similar to that of a common computer operating system. It is in the interest of all supply chain participants to agree on a standards-based tag and reader infrastructure that is interoperable. Not only does this provide the impetus for wide-scale adoption of RFID, it offers choices for end users for their method of implementation. By agreeing on a standards-based interoperable approach, the industry also avoids the fate of having to deploy more than one RFID methodology to serve the same channel to market.

How the Tag Data Security Infrastructure Works

Functional Requirements

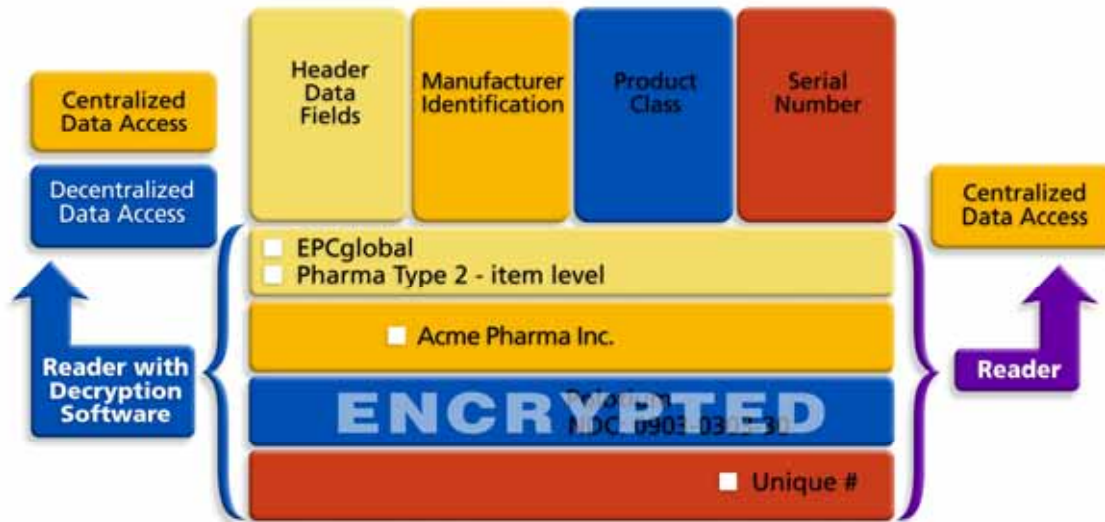
An EPC number should be programmed onto the tag as the cornerstone for pharmaceutical product identification. The Tag Data Security Infrastructure can be used to incorporate both network and off-network capabilities that support the available infrastructure in the pharmaceutical supply chain ecosystem. For example, to answer the question of where product data (NDC) should reside – on the tag or not – the TDSI can accommodate both scenarios by providing options as to how the EPC number contains product data: either encrypted on the tag or accessed through a network link. In the network scenario, a new version of an EPC numbering scheme is introduced which contains no product information in the data structure of the EPC. Here, the tag's product data is held in a central database where it is referenced by the EPC number as a unique pointer.

For an EPC numbering scheme using SGTIN with encryption, the tag's product data is digitally scrambled or signed using private key and cryptographic software in an RFID reader, and is only able to be decrypted by a reader with the appropriate corresponding public key and software. The product information can then be made available for local applications, such as smart shelves. And because the EPC number maintains its uniqueness, it can still be used as a unique pointer for network applications, like item-ePedigree.

The graphic below illustrates how the TDSI works using encryption. The 96-bit EPC SGTIN numbering scheme has four basic data elements: a header, a manufacturer ID, product class information and a serial number. Only the product class information portion of an EPC number is encrypted. This allows standard readers that have no decryption capability (gray reader on the right) to process tag EPC numbers to the EPCglobal Network for centralized data processing. Compliant readers with decryption software (green reader on the left) are able to both decrypt product data for local use and forward the tag EPC number to the EPCglobal Network. Furthermore, EPC compliant readers with decryption software can work with non-encrypted item-level tags and the EPCglobal Network.

Encrypting tag data requires special reader software and distribution of cryptographic keys. The TDSI should employ a single standardized cryptographic methodology for tags and readers, and the cryptographic approach should provide both *authentication* and *product encryption* capability.

EPC Gen 2 tag data structure with encryption



Graphic 1: EPC Gen 2 Tag Data Structure with Encryption

Elliptic Curve Cryptography (ECC) RFID Security

As stated in the previous section, a standardized cryptography method should be used as part of the Tag Data Security Infrastructure for tag encryption and authentication. The Institute of Electrical and Electronic Engineers (IEEE) has developed the IEEE Standard 1363a Elliptic Curve Cryptographic (ECC) algorithm as a new standard for public-key cryptography. The National Security Agency (NSA) has selected ECC as critical technology for protecting mission-critical national security information. NSA has defined 2 algorithm families for U.S. Government communications: Suite A and Suite B. The Suite A family is secret algorithms. Suite B is a standardized set of algorithms designed to meet U.S. Government requirements for sensitive, but unclassified, secret and top-secret levels of security. Included in Suite B are ECC for the public key and key agreement protocols, and the Advanced Encryption Standard (AES). ECC security has many benefits in RFID applications because it allows:

- Very fast signature creation ensuring no incremental delays in production line operation
- The equivalent level of security as 1,024-bit RSA encryption, while using three-fourth less of the tag memory for a digital signature
- The EPCglobal 96-bit product class information to be encrypted
- Any standard reader to read the 96-bit number from an encrypted tag, and be able to forward it to the EPCglobal Network as a "pointer"

- Readers equipped with the verification key to both authenticate the tag and decrypt the product class portion of the EPC number off-network

One of the primary advantages of ECC RFID Security for ILT is that it employs conventional levels of Integrated Circuit (IC) processing capability used in supply chain RFID tags, thus achieving a higher level of security without increasing the chip's complexity or cost. An ILT incorporating ECC RFID Security requires a 64-bit Tag Identifier (TID) and 352 bits of user memory, which includes the EPC number, digital signature, and encrypted product information. It is expected that the new ILT air interface specification will incorporate faster data exchange rates mitigating the time it takes to read and write to a tag when employing ECC RFID Security.

Achieving the Tag Data Security Infrastructure

The Tag Data Security Infrastructure is designed for flexible and secure ILT deployment throughout the supply chain. For it to become a reality, pharmaceutical manufacturers, distributors and retailers must agree on the rules, specifications and methods of deployment. The EPCglobal standards process provides a forum for both the pharmaceutical industry and the RFID technical community to share ideas and collaborate on a common course of action.

From a technical perspective, the various working groups currently in the process of defining the EPC ILT specification for HF and UHF should consider adopting the IEEE Standard 1363a ECC algorithm. To make the hardware infrastructure available to the industry, reader manufacturers and other RFID solution providers should incorporate the IEEE 1363a ECC standard into their devices as part of their product offerings.

In parallel with the introduction of the Gen 2 specification, EPCglobal established a certification procedure to address both compliance and interoperability. EPC's role in establishing an item-level specification should extend to the selection of a certifying authority for the public-key cryptographic infrastructure whose role it will be to issue certificates to authorized supply chain participants and manage the allocation of private and public keys.

Although outside the scope of the TDSI, additional security measures can be considered in the ILT standard such as password read/write and/or a kill command which would completely deactivate the tag.

Prior to the availability of new ILT standard products, pharmaceutical supply chain participants can conduct TDSI pilots using ISO/IEC 15693 standard tags and readers because they have the required 64-bit TID user memory for deployment.

Tag Data Security for ILT of High-Value Branded Goods

This paper outlines a foundation for tag data security in an infrastructure for item-level tagging that provides both networked and off-network capabilities to address the requirements of all pharmaceutical supply chain participants. It incorporates a sophisticated level of security in the supply chain while creating a more flexible approach and a range of options for implementation.

While initially developed for the pharmaceutical industry, it is an approach for item-level tagging in a secure, yet open supply chain that is applicable to a range of branded goods markets such as high-value cosmetics, apparel, sports collectables, antiques and art. In all these applications consumer

protection from a secure RFID system not only comes in the form of product safety, but in raising the level of confidence for consumers that they are getting the genuine goods.

References

1. SAP AG. (2006). Pharmaceuticals: Contracts & Chargebacks Collaborative
<http://www8.sap.com/businessmaps/182A9570F4EB11D3875B0000E820132C.htm>
2. U.S. Food and Drug Administration. (2004). Combating Counterfeit Drugs – A Report of the Food and Drug Administration. Washington, DC: page 3.
http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html
3. Pharmaceutical Research and Manufacturers of America. (2005). Electronic Authentication of Pharmaceutical Packaging and the Assurance of Public Safety: Position of the Pharmaceutical Research and Manufacturers of America. Washington, DC: page 2. <http://www.phrma.org/files/2005-05-13.1171.pdf>
4. Pharmaceutical Research and Manufacturers of America. (2005). Electronic Authentication of Pharmaceutical Packaging and the Assurance of Public Safety: Position of the Pharmaceutical Research and Manufacturers of America. Washington, DC: page 3. <http://www.phrma.org/files/2005-05-13.1171.pdf>

About the Author

Joseph Pearson is the pharmaceutical business development manager for Texas Instruments RFid Systems. In his 15 years in the RFID market at TI, he has held a variety of sales, marketing and business development roles. He was instrumental in the development of several RFID patents including the ExxonMobil Speedpass™.

About Texas Instruments RFid Systems

Texas Instruments is an industry leader in radio frequency identification (RFID) technology and the world's largest integrated manufacturer of RFID tags, smart labels and reader systems. With more than 500 million tags manufactured, Texas Instruments RFid Systems' technology is used in a broad range of applications worldwide including automotive, document tracking, livestock, product authentication, retail, sports timing, supply chain, ticketing and wireless payment. TI is headquartered in Dallas, Texas and has manufacturing, design or sales operations in more than 25 countries. Texas Instruments is traded on the New York Stock Exchange under the symbol TXN. For more information, contact TI-RFid Systems at 1-888-937-6536 (North America) or +1 972-575-4364 (International), or visit the Web site at www.ti-rfid.com, or the main company site at www.ti.com.

Note: If you make physical copies of this document, or if you quote or reference this document, you must appropriately attribute the contents and authorship to Texas Instruments Incorporated. While every precaution has been taken in the preparation of this document, Texas Instruments Incorporated assumes no liability for errors, omissions, or damages resulting from the use of the information herein. Products or corporate names may be trademarks or registered trademarks of other companies and are used only for the explanation, without the intent to infringe.

©2006 Texas Instruments Incorporated
ALL RIGHTS RESERVED

Important Notice: The products and services of Texas Instruments Incorporated and its subsidiaries described herein are sold subject to TI's standard terms and conditions of sale. Customers are advised to obtain the most current and complete information about TI products and services before placing orders. TI assumes no liability for applications assistance, customer's applications or product designs, software performance, or infringement of patents. The publication of information regarding any other company's products or services does not constitute TI's approval, warranty or endorsement thereof.