

When used in conjunction with item-level tagging of drugs and other products, TDSI can protect consumer privacy while raising confidence that customers are getting genuine goods.

Dec. 18, 2006—There is widespread agreement in the pharmaceutical industry that radio frequency identification will play a critical role in creating consumer confidence in the authenticity of prescription drugs, especially as the number of counterfeit, gray-market and diverted products continues to climb. RFID technology, combined with a secure tag and data infrastructure, offers both package authenticity and pedigree.

RFID tags applied at the case and item levels to products traveling in a secure supply chain raise the confidence that products are genuine on two fronts: by determining the authenticity of the packaging, and by automating traceability to create an itemized electronic pedigree, or record, as products pass from one authorized entity to another.



While manufacturers, distributors and retailers are collaborating on RFID pilots, they're not all on the same page when it comes to the methods of deployment. One core issue is whether RFID data should be centralized, decentralized or both. Should product information be associated with the tag on the network, or off? If product information resides on the tag, how can a company protect consumer privacy? The ultimate success of either or both of these deployment options may depend on a Tag Data Security Infrastructure (TDSI). A TDSI provides a broader and more flexible approach for a secure supply chain, encompassing all stakeholder requirements while providing a range of implementation options.

Tag Data Security Infrastructure—What and Why

Believe it or not, having deployment "options" within a "standard" item-level tagging infrastructure is not an oxymoron. The TDSI is a set of rules, specifications and common protocols allowing item-level tags and readers to work across the industry's information technology ecosystem. It always supports network-based applications, and it bridges the pharmaceutical centralized/decentralized data structure divide 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, or NDC) on the tag, how to authenticate products, methods of ensuring consumer privacy and how to secure tagged products at the case, pallet and item levels.

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](#) specification development process.

How the Tag Data Security Infrastructure Works

An EPC number programmed on the tag is the cornerstone for pharmaceutical product identification. The TDSI can be used to incorporate both network and off-network capabilities to support the pharmaceutical supply chain infrastructure.

For example, in regard to where product data should reside—on the tag or off—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. For an EPC numbering scheme using a Serialized Global Trade Identification Number (SGTIN) with encryption, the product-data portion of the tag's EPC number is digitally scrambled and can be decrypted only by a reader with the appropriate corresponding cryptographic software. The product information is then 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 an item-level electronic pedigree. Any standard interrogator can read the 96-bit EPC number from an encrypted tag, then forward it to the EPCglobal Network as a "pointer." Readers equipped with the verification key can both authenticate the tag and decrypt the product-class portion of the EPC number off-network.

Elliptic Curve Cryptography (ECC) RFID Security

A standardized cryptography method is a vital part of the TDSI for both tag-data encryption/decryption and authentication. Meeting these goals is a new public-key cryptography standard: the [Institute of Electrical and Electronic Engineers'](#) (IEEE) Standard 1363a Elliptic Curve Cryptographic (ECC) algorithm. The [National Security Agency](#) (NSA) has selected ECC as critical technology for protecting mission-critical national security information. For RFID applications, ECC enables very fast signature creation, ensuring no incremental delays in production-line operation. The IEEE Standard 1363a ECC algorithm provides the equivalent level of security as 1,024-bit RSA encryption, but uses 75 percent less tag memory for a digital signature. What's more, ECC's efficiency provides a high level of security to supply chain RFID tags without increasing computing power, complexity or cost.

The Path to a Tag Data Security Infrastructure

The TDSI is designed for flexible and secure item-level tagging 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.

From a technical perspective, the working groups in the process of defining the EPC item-tagging specification for high-frequency (HF) and ultrahigh-frequency (UHF) could consider adopting the IEEE Standard 1363a ECC algorithm. To make the hardware infrastructure available to the industry, reader manufacturers and other RFID solution providers would 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. The organization's role in establishing an item-level specification could 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 item-tagging standard, such as a password-protected read-write command and a password-protected kill command that would completely deactivate the tag.

A TDSI can be the security foundation for item-level tagging that provides both on- and off-network capabilities to address the requirements across the pharmaceutical supply chain. It incorporates a sophisticated level of security in the supply chain, while creating a more flexible approach and a range of options for implementation.

This approach to item-level tagging for the pharmaceutical industry in a secure, yet open supply chain is applicable to a range of high-value branded goods from cosmetics and apparel to sports collectables, antiques and art. In all of these applications, consumer protection from a secure RFID system not only comes in the form of product safety, but in raising consumers' confidence that they are getting genuine goods.

Joseph Pearson is the pharmaceutical business development manager at [Texas Instruments](#).