Securing the Pharmaceutical Supply Chain with RFID and Public-key infrastructure (PKI) Technologies

Joseph Pearson, Pharmaceutical Business Development Manager

Texas Instruments Radio Frequency Identification (TI-RFid™) Systems

Executive Summary

To combat the problem of counterfeit and compromised drugs, this paper introduces a new approach for advancing the security of the pharmaceutical supply chain and improving patient safety. This approach is built on existing industry standards and adds a new layer of authentication to pharmaceutical drugs in the supply chain to create an **Authenticated radio frequency identification (RFID)** capability at the item level. **Authenticated RFID** combines globally accepted and deployed ISO/IEC standards for RFID and Public-key infrastructure (PKI) technologies. The result is elevated confidence in the security of the pharmaceutical supply chain as item-level authentication is combined with validated chain-of-custody transactions.

The **Authenticated RFID** model can immediately impact pharmaceutical supply chain safety through real-time, off-network authentication at the dispensing pharmacy, a first step that can be implemented quickly with minimal investments in current infrastructure (See Figure 1). As the model is subsequently adopted throughout the pharmaceutical supply chain, the robust architecture supports an extensive electronic pedigree (ePedigree) system with multiple layers of electronic and physical security.

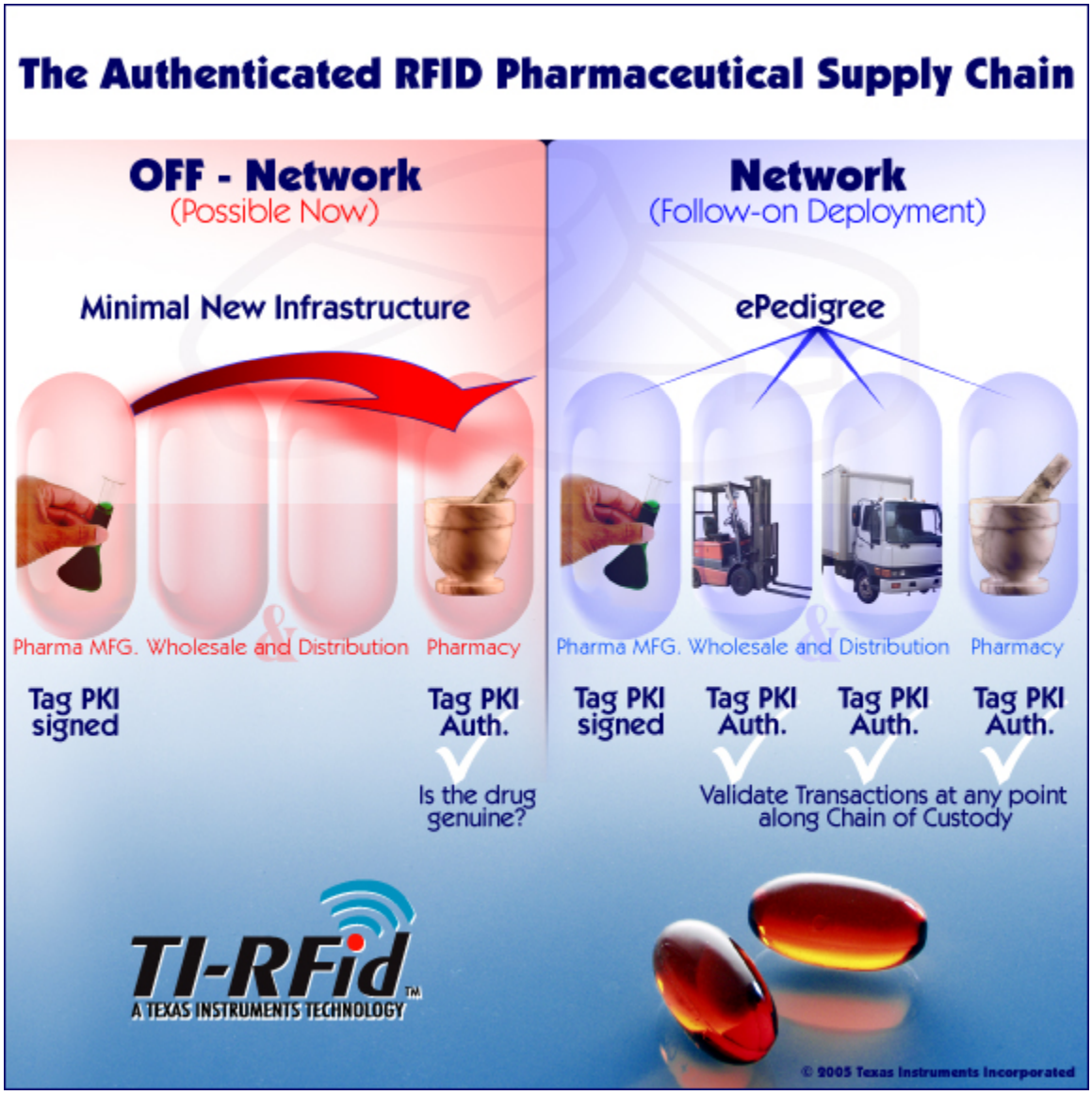

Figure 1: Authenticated RFID Deployment

Counterfeit Drugs in the Public Health Supply Chain

Counterfeit and compromised drugs are increasingly making their way into the public healthcare system and are considered a threat to the public health by the Food and Drug Administration (FDA).[1] Counterfeit pharmaceuticals are a $32 billion dollar industry representing 10 percent of the global market, according to the FDA. The recent increase in patients in the U.S. receiving fake or diluted drugs is focusing more attention on the need for drug authenticity. In 2004, the FDA reported 58 counterfeit drug cases – a 10-fold increase since 2000.[2]

Compounding this issue is a complex pharmaceutical distribution infrastructure that makes it difficult to ensure supply chain integrity as products move from point of manufacture to point of dispensing. How can all of the participants in the pharmaceutical supply chain assure their customers safe and authentic products by closing the gaps in supply chain integrity, while also securing their brand, reputation and financial performance?

The FDA recently reiterated its belief that RFID is "the most promising technology" in developing an electronic safety net by 2007.[3] And a recent white paper by The Pharmaceutical Research and Manufacturers of America (PhRMA) detailed how electronic authentication technology can be implemented in a timely manner.[4] PhRMA "believes that the interests of patient safety in securing the drug supply are too important to delay electronic authentication at the dispensing level while extensive "electronic pedigree" systems are developed."[5]

In addition, a recent survey of 225 pharmaceutical executives worldwide commissioned by Ernst & Young and conducted by the Economist Economic Unit suggests that manufacturers, wholesalers and pharmacists alike agree that the "most effective deterrents for diversion (and counterfeiting) are likely to be internal operating procedures, product security controls and new tracing technologies."[6] Among the techniques used to safeguard the supply chain include a review and modification of internal processes and controls, third-party vendor and customer audits, ceasing to do business with a vendor or customer violating the law or contract requirements, and installing a new technology, such as radio frequency identification (RFID) Electronic Product Code (EPC) systems.

The retail industry, led by EPCglobal Inc™, has shown that RFID provides the potential for automated track and trace capabilities and allows real-time visibility into where the product is at all times. In the pharmaceutical industry, the counterfeiting problem and resulting threats to patient safety demand an additional requirement for item-level authentication to determine whether or not a product is genuine. By adding a new layer of integrated security combined with RFID technology, manufacturers can greatly increase a patient's confidence that a drug is authentic. The **Authenticated RFID** model supports the efforts of the EPCglobal, Inc and although it is not a formal extension of EPCglobal standards, it attempts to leverage EPCglobal infrastructure in order to proactively address the need for item-level authentication.

The Authenticated RFID Model – An Overview

The **Authenticated RFID** model enhances item-level product security in real-time, independent of a connection to a host network, by creating strong authentication between the tag and an Authenticated RFID reader. By initially deploying the model at the point of manufacturing and the point of dispensing, the pharmaceutical industry immediately provides a higher level of item-level authentication against counterfeit

products. After initial introduction of RFID and PKI end-to-end item-level authentication, the integration of other points in the chain of custody provide ever increasing levels of confidence in the supply chain.

Well established ISO/IEC 13.56 MHz standard RFID plus standards-based public key technology, digital signatures and data encryption are used by the **Authenticated RFID** model to validate that a tag originating from the pharmaceutical manufacturer is genuine and enables enterprises to create an additional layer of supply chain validation by associating event data written on the tag to the networked supply chain application. Because the **Authenticated RFID** model is based on proven, open security algorithms, the integrity of the systems does not rely on proprietary security which runs a greater risk of being compromised.

Multi-Tiered Approach Against Product Counterfeiting and Diversion

The new solution, from Texas Instruments and VeriSign, Inc. brings together a combination of hardware and a service-based architecture to provide manufacturers with multiple lines of defense in addressing the issue of product counterfeiting and diversion.

1. **Secure and Unique Tags Created for Each Pharmaceutical Manufacturer**
   The **Authenticated RFID** model's multi-layered transaction-based security approach begins with the ISO/IEC standard RFID transponder. The transponder manufacturer programs and locks into the chip's silicon a Unique Identifier (UID) number also known as the Unique Item Identifier (UII), as well as the Product Manufacturer Identifier (PMID) number similar to a Labeler Code to create a secure and unalterable code for each tag.

2. **Digital Signing of Tags**
   During the tag-to-label or tag-to-package conversion, a 1,024-bit digital "signature" is generated and locked into the tag's memory. A digital signature can be read by **Authenticated RFID** readers to "validate" the tagged product as it moves through the supply chain, provided the reader is supplied with the appropriate manufacturer public "key" to read the signature. The use of standards-based public key technology, digital signatures, data encryption, and implementation of best practices helps to ensure the authenticity of the signature, and, consequently, the authenticity of the tag itself.

   The value added by the use of the digital signature is that it creates a unique manufacturer "electronic fingerprint" on the RFID tag – which can be further coupled to physical elements of the label. [For more information on additional aspects of pharmaceutical **Authenticated RFID** label security, refer to an upcoming white paper written by CCL Label, Inc.]

3. **Supply Chain of Custody Event Validation**
   Throughout the supply chain, **Authenticated RFID** readers are designed to first authenticate a tag digital signature, and then create event validation information for both the tag and data network.

   Starting with the production data, supply chain event information is provided via the host application to a network and is associated with the tag information. As the tag moves through the supply chain, the **Authenticated RFID** reader has the capability to record additional events to the tag. These events are date/time stamps and are stored on the tag as event markers, and they do not contain any product or location information. This capability allows for another level of authentication when comparing the event data written to the tag to corresponding event data stored in a distributed data network.

The **Authenticated RFID** reader may also have the capability to digitally sign the event data stored in the network to further increase the difficulty of falsifying, modifying or recreating the network stored events and corresponding markers on the tag.

Point of Dispensing – Pharmacy Provides Customer a Genuine Product

One of the significant benefits of accurately authenticating the tag at the item level is the protection of patient safety. Integrating a digital signature on the RFID tag adds an important layer of security. Even if no events have been captured after the product leaves the manufacturing facility, it is still possible at the point of dispensing to significantly increase the confidence that the tag was originated at an authentic pharmaceutical manufacturer.

With the participation of additional points within the supply chain, higher levels of confidence can be achieved by comparing events stored on the tag to associated data stored in a distributed data network. Adoption and recording of events in all nodes within the pharmaceutical supply chain will happen over time. Nonetheless, every piece of additional captured data augments the tag digital signature and decreases the likelihood that the pharmaceutical is counterfeit.

Components of the Authenticated RFID Model

Radio Frequency Identification (RFID)

In its most basic form, RFID uses a semiconductor (microchip) in a tag or label to store data. The data is transmitted from, or written to the tag or label via radio signals (within a defined range) of the correct frequency and with the correct communications protocols. An RFID reader broadcasts a signal through an antenna to a transponder (consisting of a microchip and antenna) which receives the signal and is charged with

enough energy to send back an identifying response. A read/write tag can be updated with new data many times. The RFID reader sends the tag data to a computer system for collecting, logging and processing.

The RFID Transponder's Unique Identifier (UID) and Product Manufacturer Identifier (PMID)

Storage of data on an RFID transponder or tag is divided into different blocks or segments of memory. One segment of the RFID chip's memory is reserved for the Unique Identifier (UID). The UID consists of a RFID tag vendor number and a number unique to the individual chip. It is etched into the silicon and is locked at the point of chip manufacturing so that the chip cannot later be changed.

In addition to the UID, **Authenticated RFID** transponders are also programmed with a Product Manufacturer Identifier (PMID) number by the RFID tag manufacturer. The PMID is a new concept introduced by the **Authenticated RFID** model and equates to the pharmaceutical manufacturer's Labeler Code as found in the National Drug Code (NDC) number or any other manufacturer selected schema. Similarly to the UID, the PMID is locked by the RFID manufacturer creating an unalterable code.

ISO/IEC Standards-Based 13.56 MHz High-Frequency Technology

The **Authenticated RFID** model is based on 13.56 MHz technology that is compliant with the globally accepted ISO/IEC 15693 and ISO/IEC 18000-3 Mode 1 standards. The International Standards Organization (ISO) and the International Electrotechnical Commission (IEC) have established a number of global standards that use 13.56 MHz High-Frequency (HF) RFID technology. ISO/IEC 15693 is the standard for contactless vicinity cards, and is used for a variety of item-level asset tracking applications. Although it's a vicinity card standard, the applications of the ISO/IEC 15693 standard covers a number of different form factors, including both flexible RFID smart inlays and smart labels. The ISO/IEC 18000 protocols were designed as the global standard for RFID item-level tracking in supply chains. ISO/IEC 18000-3 is the air interface protocol for 13.56 MHz. The air interface protocol defines how the tag and reader communicate.

There are a number of advantages using RFID technology operating in the HF band of the electromagnetic spectrum versus using Ultra-High-Frequency (UHF) RFID technology. HF's shorter read range allows for more defined read zones better suited for item-level applications. HF works more effectively around metal and is better able to penetrate water and other liquids. The 13.56 MHz frequency occupies an International Scientific and Medical (ISM) band, which is available worldwide.

Authenticated RFID Readers

Unlike a standard RFID reader, the **Authenticated RFID** reader is PKI-enabled and is also compliant with ISO/IEC 15693 and ISO/IEC 18000-3 standards. It is used by authorized pharmaceutical supply chain participants, starting with the pharmaceutical manufacturer. Access to the network connection via the Internet for periodic public-private key pair updates will be required for most **Authenticated RFID** readers.

The **Authenticated RFID** reader performs the following four functions:

1) Authenticates tags that are presented using digital signature verification techniques
2) Programs the chain-of-custody event marker to tags that are presented
3) Creates a digital signature using the reader's private key
4) Communicates relevant event information, including digital signatures and event markers to the local computer system

The local computer system receives the information about the tag from the **Authenticated RFID** reader and provides external distributed data network access to the required information about the tag data and the particular supply chain events. [For more information on **Authenticated RFID** reader technology and physical security technologies, see the upcoming white paper written by 3M.]

Public-key Infrastructure (PKI) and Digital Signatures

Public-key infrastructure is a security architecture that combines software, encryption technologies and services that enable enterprises to protect the security of their communications and business transactions.[7] In the pharmaceutical supply chain, a PKI infrastructure provides a protected environment for safe information exchange at every stage.

PKI relies on public key cryptography which uses a pair of mathematically related cryptographic keys – a public key and a corresponding unique private key.[8] While the keys are mathematically related to each other, it is computationally infeasible to calculate one key's encryption from the other when using a 1,024-bit key size. The public key is freely distributed; the private key is kept private. The **Authenticated RFID** model uses a private key to generate a digital signature for a particular tag, which is authenticated using a public key. A digital signature is a unique "stamp" placed on the data which assures that the originator, and therefore the message or product, is genuine.

The PKI methodology applied in the **Authenticated RFID** model consists of two types of cryptographic security algorithms for digital signatures:

Secure Hash Algorithm 1 (SHA-1) was developed by the U.S. National Security Agency in 1995. It is commonly used to generate hashes or unique strings of values that are used to encrypt and decrypt digital signatures.

The RSA Cryptosystem, named after its inventors Ron Rivest, Adi Shamir and Leonard Adleman, allows encryption and authentication to take place without the sharing of private keys. Anyone can verify a signed digital message, but only someone in possession of the correct private key can create or sign a digital message.[9] The **Authenticated RFID** model specifies a 1,024-bit key size that provides an extremely high level of security.

Authenticated RFID and the PKI Process

The **Authenticated RFID** solution uses a tag digital signature to ensure that the tag is genuine to a specific pharmaceutical manufacturer and is not counterfeit.

As shown in Figure 2, the UID and PMID are the basis for the message to be encrypted. The steps to generate a tag digital signature are to first read a tag and then condense the data with a SHA-1 Hash algorithm into a few lines which are called the message digest. The **Authenticated RFID** reader uses its private key to encrypt the message digest resulting in the digital signature, which is then written and locked into the tag memory.

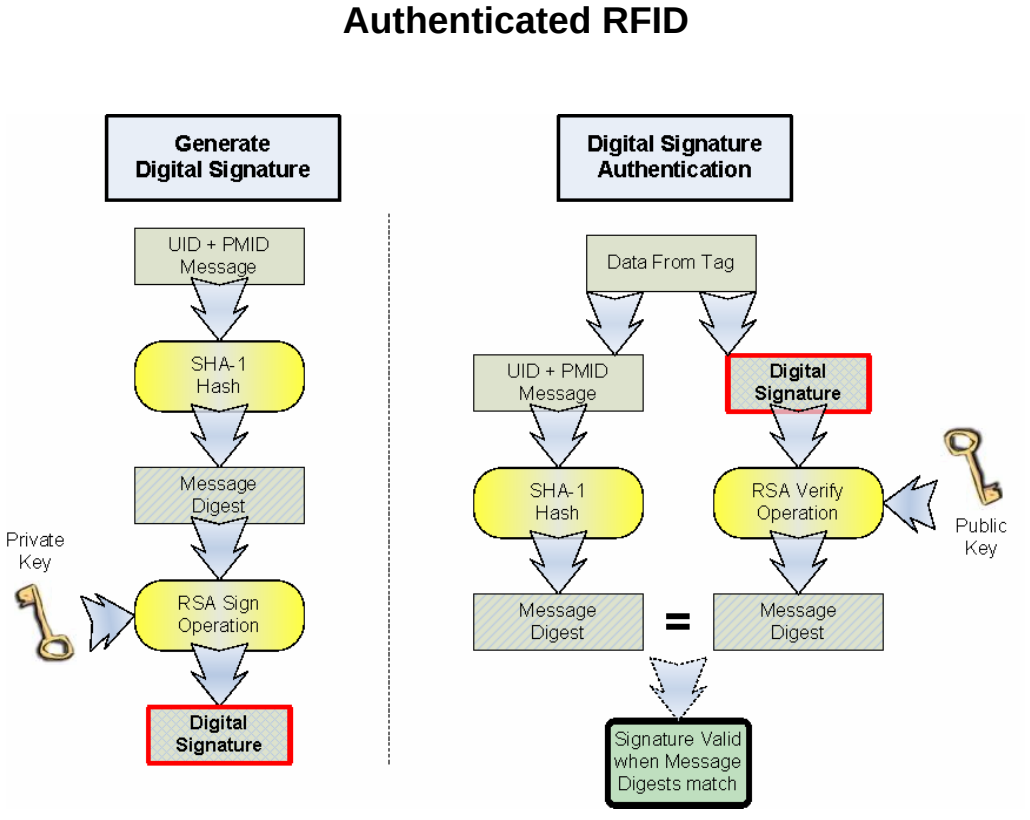

Figure 2: Signature Generation and Authentication Using PKI

To authenticate a tag's digital signature, an **Authenticated RFID** reader obtains the tag data and performs two separate calculations for comparison. One calculation is a repeat of the above step to create the message digest using the SHA-1 Hash algorithm. The other calculation is to decrypt the digital signature with a public key to reconstitute the message digest. The tag's PMID identifies the correct public key when decrypting the tag digital signature. If the message digest numbers are equal from the separate calculations, then the tag is genuine.

Event Markers and Network-Hosted Digital Signatures

The **Authenticated RFID** model provides an additional level of authentication when the date and time of a supply chain event is recorded by the **Authenticated RFID** reader and is programmed onto the tag as the event marker. This establishes a strong relationship between the tag and distributed data network through the event marker. The event marker is permanently programmed onto the tag and is also made available through the network at each chain-of-custody event in the supply chain. The event marker, using the date and time of the event, provides an inseparable link and look-up index between the supply chain event, tag and the corresponding external information.

In addition to the event marker, the **Authenticated RFID** reader creates a digital signature for each supply chain event. This digital signature verifies that the reader and event have not been changed or tampered with and allows for an additional level of reader security. The **Authenticated RFID** reader uses its own private key to create the event digital signature. **Authenticated RFID** readers are controlled and governed by supply chain participants to accurately represent the authorized actions of the organization.

The network based information for the event and corresponding digital signature can be integrated into existing electronic pedigree processes. This allows for unparalleled levels of assurance that the transactions among the pharmaceutical manufacturer, the wholesalers/distributors and final delivery to the pharmacy have all occurred in a safe and secure supply chain.

Distribution of Public and Private Keys

The **Authenticated RFID** reader stores its own private and public keys in secure tamper-resistant mechanisms. The distribution of key pairs for the **Authenticated RFID** solution is standards based and leverages the successful distribution processes already widely used in markets such as the cable modem industry.

The important element in issuing the private and public key certificates to the **Authenticated RFID** readers is to ensure that all of the certificates come from a trusted source. To that end, a trust hierarchy is used to issue the keys, with the root certifying authority policy managed by an industry organization such as Secure Access for

Everyone (SAFE) and EPCglobal Inc. [For more information on public/private key distribution and supply chain security, refer to an upcoming white paper written by VeriSign Inc.]

Conclusion

The pharmaceutical industry is addressing the very real threat to patient safety from counterfeit medicines. The combination of RFID and PKI technologies in the **Authenticated RFID** model is an immediate and vital step forward in securing the pharmaceutical supply chain. The safety of medicines can be ensured and the immediate danger of counterfeit medicines reduced by implementing real-time authentication at the dispensing pharmacy.

The **Authenticated RFID** solution advances RFID beyond track and trace visibility to true, transaction-based security of each product at every stage along the supply chain process. Working independently of a connection to a networked system, offline between the tag and the reader, the model assures item-level authentication to determine product legitimacy. In addition, the use of event markers and event digital signatures empowers pharmaceutical ePedigree software with information to create an indisputable link between the supply chain event and the network infrastructure.

The **Authenticated RFID** solution endorsed by industry leaders including Texas Instruments, VeriSign Inc., 3M, and CCL Label, Inc., provides the pharmaceutical market with a new authentication solution that advances the integrity of the supply chain to help ensure consumer safety.

References

1. Combating Counterfeit Drugs: A Report of the Food and Drug Administration Annual Update, May 18, 2005, page 1. Available at http://www.fda.gov/bbs/topics/NEWS/2005/NEW01179.html
2. Ibid, page 2
3. Ibid, page 3
4. Electronic Authentication of Pharmaceutical Packaging and the Assurance of Public Safety: Position of the Pharmaceutical Research and Manufacturers of America, May 12, 2005, page 1. Available at http://www.phrma.org/publications/policy//admin/2005-05-13.1171.pdf
5. Ibid, page 2
6. Pharmaceutical Sector at a Crossroads in Public Trust According to Ernst & Young 2005 Global Pharmaceutical Report, press release, Available at http://www.ey.com/global/content.nsf/US Media_-_Release_-_04-28-05ADC
7. Understanding PKI, VeriSign, Inc. Available at http://verisign.netscape.com/security/pki/understanding.html
8. ArticSoft Introduction to Public Key Infrastructure, Available at http://www.articsoft.com/wp_pki_intro.htm
9. RSA Laboratories What is the RSA cryptosystem? Available at http://www.rsasecurity.com/rsalabs/node.asp?id=2214

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.