TEXAS INSTRUMENTS

RFIDHF01—August 2006
White Paper

Increasing Security in the Supply Chain with Electronic Security Markers

Joseph Pearson, Business Development Manager
Texas Instruments Radio Frequency Identification (TI-RFid™) Systems

Executive Summary

Controlling the legitimacy and the brand integrity of a product in the supply chain has been a struggle for manufacturers long before the first knock-off Rolex watch. However, a new twist on using radio frequency identification (RFID) may provide an answer. Smart electronic security markers, based on RFID technology, are making an impact with item-level security and laying the ground work for this kind of protection in future applications. RFID tags embedded at the product item-level make it easier to guarantee authenticity and represent an increasingly important value proposition for RFID by protecting product and brand integrity.

This paper will take a look at the size and most common means of counterfeiting today in pharmaceutical and consumer products industry as well as with peripheral or replacement market products. It will then explain how an RFID system works and propose a range of increasingly secure methods of using RFID to prevent some of the different types of counterfeiting.

Counterfeiting Continues to Grow

Counterfeiting has become a worldwide problem that has reached “epidemic proportions,” according to DNA Technologies in their report entitled "The 21st Century Solution to Counterfeiting, Forgery & Diversion"[1]. DNA Technologies estimates that in addition to the elimination of more than 750,000 jobs, American businesses lose more than $200 billion in revenues every year. This does not take into account activity in other areas of the world which can reach up to five to eight percent of the total world trade.

One of the problems in addressing counterfeiting is that it can take different forms in the supply chain at the item-level or through diversion. The most prolific abuse is the counterfeited product at the item level, for example brand name apparel, electronics and pharmaceutical products (Figure 1).

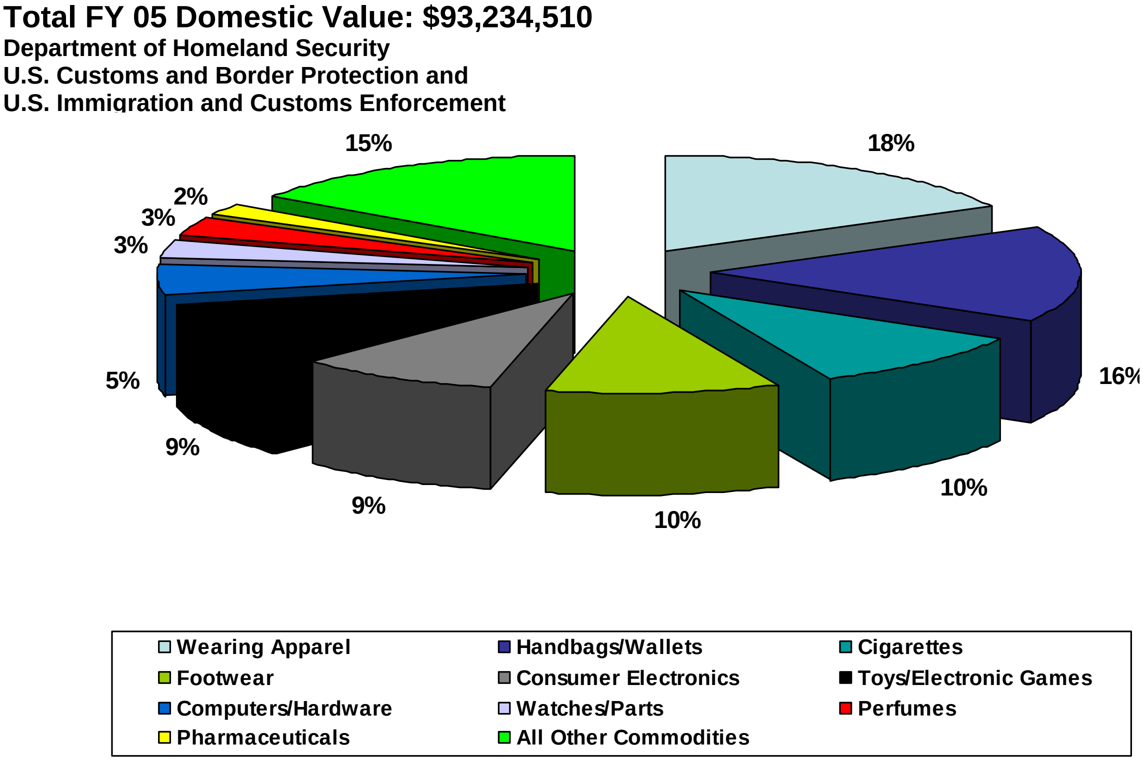

Figure 1: Chart showing counterfeit products seized in 2005 by U.S. Customs and Border Patrol

Another growing problem is counterfeit and compromised drugs, which are increasingly making their way into the public healthcare system and have been identified as a threat to the public health by the Food and Drug Administration (FDA). In 2004, the FDA reported 58 counterfeit drug cases – a 10-fold increase since 2000.[3] In China it was estimated that in one year a total of 192,000 Chinese patients died from fake drugs while in Nigeria, almost 2,500 people were killed through injecting a supposed anti-meningitis drug during an international vaccination campaign.

Another example of counterfeiting at the item level is with peripheral electronics equipment such as replaceable ink printer cartridges. Since a manufacturer usually earns the highest margin for a system from the peripherals or replacement goods, counterfeit peripherals impact the manufacturer's profitability. Counterfeit peripherals can also cause problems with the quality and operational performance of the system.

Diversion is the use of an unauthorized channel in the supply chain and is another form of counterfeiting. Branded cosmetics sold at flea markets by unauthorized vendors or pharmaceutical products purchased at a senior citizen discount to unqualified individuals are examples of diversion. Diversion typically occurs because of differentiated price structures within an intended channel or between market segments with different qualifications. Channel corruption within the supply chain can distort profits and revenue distribution which often leads to additional black market activities and diminished brand value.

Current Anti-Counterfeit Methods

Current approaches to address counterfeiting can be classified as either overt or covert packaging technologies. Overt technologies on packages are visible to the eye and include methods such as optical variable inks which are colors that shift as the user moves the package between various viewing angles or tamper-proof/tamper-evident techniques which show package manipulation such as plastic covering the cap on medicine bottles.

Covert technologies are integrated into packaging and are invisible to the naked eye and include such methods as ultraviolet/infrared light elements which can only be detected with special equipment or microscopic nanotext / images which are complex printing that is hard to replicate.

Whether overt or covert methods are utilized, the need for human involvement remains an overriding requirement for their use. In many supply chain scenarios, everyone in the supply chain --from receiving clerks to stockers to check out clerks ---is required to be aware of the overt method used. Due to the complexity and the number of touch points in the system, this often leads to anti-counterfeit tactics which are ignored, compromised or not utilized in a way to make them fully effective. Therefore, covert and overt approaches are often used **after** there is already a suspicion that a problem exists.

How RFID Works

RFID technology enables new ways to prevent illegitimate products, peripherals and channels from occurring. In order to understand how this works, we must understand how an RFID system operates.

A typical RFID system is comprised of three main elements, which include an RFID tag, a reader and a host processor.

The RFID system uses a microchip in an RFID transponder (tag) to store and transmit data via radio signals. Through a transponder's antenna, the tag receives an electromagnetic signal at the appropriate frequency from an RFID reader. The passive tag (meaning it has no battery) is charged with enough energy to communicate with the RFID reader and provide the reader with the data stored on the tag.

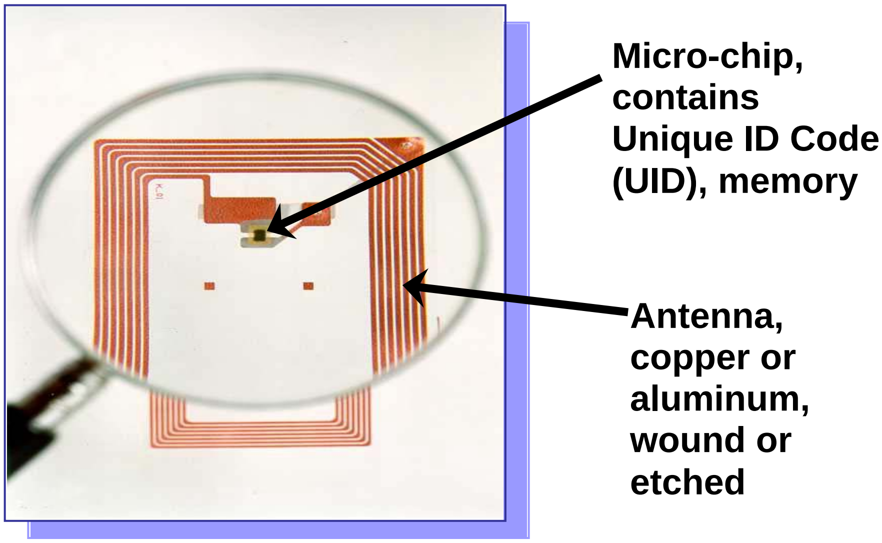
Micro-chip, contains Unique ID Code (UID), memory
Antenna, copper or aluminum, wound or etched

Figure 2: Micro-chip and antenna: significant elements of an RFID transponder (tag)

RFID for Protecting Products

RFID removes the propensity for counterfeiting through human involvement by providing an embedded electronic security marker that is automatically read as it passes through the supply chain either individually or as a group inside a shipping case. An electronic security marker is a unique data code that, by itself or in conjunction with a network, can distinguish the product as genuine. This marker is unique to the individual product and cannot be easily altered, providing an enhanced level of security. Combined, the attributes of being both automated and highly secure gives an electronic security marker many advantages over traditional covert and overt marking techniques.

In peripherals, if the security marker on the tag is identified as legitimate by the host processor, then the product is accepted in the application. As the product travels through the supply chain, the electronic security marker is picked up by RFID readers which authenticate the products as genuine. The authentication happens either directly between the RFID reader and tag, or by retransmitting the data to a network system and validating the information.

On- or Off-Network Authentication

The authentication method of the tag data could be either on- or off-network. As an example of an on-network solution, EPCglobal Inc™ is creating an Electronic Product Code (EPC) item-level serialization scheme for item-level tags. This will serve as an electronic security marker unique to each product. The vision is for products to have automated track and trace capabilities as well as real-time visibility of the product through the EPCglobal Object Name Service (ONS) Network. The EPCglobal ONS will act as a traffic cop and direct authorized network inquiries to the correct data base hosting the desired data.

The off-network method enables RFID readers to authenticate the tag through a shared data encryption algorithm. For example, an electronic security marker can be a digital signature generated via a public-key infrastructure (PKI) and programmed into the tag's memory. An RFID reader is able to validate the tagged product because the reader is supplied with the appropriate manufacturer public key to authenticate the digital signature. PKI relies on public key cryptography which uses a pair of mathematically related cryptographic keys – a public key and a corresponding unique private key. While the keys are mathematically related to each other, given proper key length, it is computationally infeasible to calculate one key's encryption from the other. For example, when using RSA encryption, a 1,024-bit size digital signature will prohibit a brute force attack to gain knowledge of the cryptographic private key.[4]

By using a digital signature, a manufacturer's unique "electronic fingerprint" is created and programmed into the RFID tag, which can then be authenticated by an RFID reader without a network.

Real world examples and benefits of item-level RFID integration

There are already several examples of RFID item-level tagging being used to protect product integrity. These cross various industries and address the problems of illegitimate products and channels.

Medical

RFID electronic security markers are used in a variety of medical equipment systems such as ventilators to ensure that authentic peripheral products are used with the host system. Typically, RFID reader chip sets are built into medical equipment and are used to read tagged peripheral products as they are connected. In the case of a respirator, the ventilator's host processor authenticates that the correct flow sensors are installed prior to operation.

The benefit is first and foremost patient safety. Having the correct peripheral with the appropriate medical equipment ensures the parts will operate together as they were designed, which could be a matter of life or death. Additional benefits include product authentication, automated calibration, and set-up information in various medical equipment which are RFID-enabled.

Clothing

RFID electronic security markers can be used to protect and manage clothing at retail stores. For example, the British retailer Marks & Spencer plans to tag clothing apparel at the item-level in six clothing departments at 53 stores in 2006. Marks & Spencer must manage 40 size variations for every man's suite and 68 size variations for every woman's bra.[5]

Tagging high-end clothing also helps to prevent diversion in the supply chain, which in turn protects product and brand integrity. With item-level tagging, name brand clothing and accessories are distinguishable from a knock-off and if a legitimate item is diverted from the supply chain, it can be verified with the security marker and traced back to the point of diversion.

Pharmaceutical

Patient safety is a driving force behind pharmaceutical item-level tagging. RFID will enable track and trace capability through the EPCglobal ONS networks and/or direct authentication with off-network RFID readers. As more products are tagged, supply chain efficiencies will occur at the manufacturer, wholesaler and pharmacy.

Purdue Pharmaceutical applies RFID to each 100-count bottle of their painkiller OxyContin to fight counterfeiting while Pfizer announced a pilot in which they are applying RFID tags to bottles of Viagra sold in the U.S. Other pharmaceutical manufacturers are evaluating RFID on production items. The package can use a label that contains an RFID tag. The tag would include a digital signature security marker that would be authenticated directly by RFID readers prior to being dispensed to patients.

Electronics

Similar to medical equipment, electronic products can be enabled with RFID security markers to protect peripheral authenticity. Many electronic systems rely on peripheral products in order for the system to perform as intended. Fake peripheral products can lead to damage or inadequate quality. For example, counterfeit ink cartridges for printers can lead to damaged printer heads because of thick viscosity in the counterfeit liquid ink. RFID tags can be embedded into the ink cartridges to ensure that only the correct consumable replacements are used in printers.

Another use of RFID for electronic products is reverse logistics - product returns. Too often, electronic retailers are stuck with counterfeit or damaged goods when they are returned to stores by dishonest patrons. An electronic security marker ties the relationship of a particular product to a given sale and then to the return.

Manufacturers could benefit from the elimination of fraudulent products being returned to retailers by placing item-level RFID tags on their high end products and components. Additionally, host system performance and overall profitability can be assured through electronic security markers embedded into peripheral consumable replacements.

Beauty products

RFID tags are being integrated into beauty products to protect their sales channel, which is an integral element to the success of the business model. For example, it is important for a high profile cosmetic brand sold through direct sales, not to be undermined by some of the product being diverted and offered by street vendors. This can occur when higher volume discounts are awarded to persons in the supply chain who buy extra product quantities in order to get better pricing. Then the excess products are “dumped” at cost to non-authorized channels.

RFID tags embedded in the product packaging are read by handheld units to identify the diverted product being offered through street vendors. The electronic security markers indicate the product pedigree, leading to the discovery of where the improper channel diversion occurred.

Conclusions

Protecting product and brand integrity presents a daunting challenge as the problem of counterfeiting continues to grow. Counterfeiting not only affects the bottom line of businesses causing job loss, but it can also cause loss of life when fake drugs are introduced into the market.

With its ability to provide item-level tagging, protecting product and brand integrity is set to become the new value proposition for RFID. Controlling the legitimacy of a product in the supply chain may become a non-issue for manufacturers as the use of electronic security markers helps control counterfeiting at the item and product level.

References

1. http://www.dnatecaus.com/counterfeit.htm
2. http://www.cbp.gov/linkhandler/cgov/import/commercial_enforcement/ipr/seizure/fy05_midyear_stats.ctt/fy05_ipr_midyear.pdf
3. 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
4. Securing the Pharmaceutical Supply Chain with RFID and Public-key infrastructure (PKI) Technologies; By Joseph Pearson; Texas Instruments RFid Systems
5. http://www.informationweek.com/story/showArticle.jhtml?articleID=60402017

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.

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.