



Protecting Against Counterfeits, Generics and Substitutes with RFID

March 21, 2007

Table of Contents

Table of Contents	2
Introduction	3
The Counterfeiting Epidemic	3
Beyond Counterfeiting: Generics and Substitutes.....	4
The Toll of Counterfeits, Substitutes, and Generics.....	4
The Benefits of RFID-Based Product Authentication	5
How RFID Works	6
Picking the Right RFID Solution for Product Authentication.....	7
Example 1: Equipment and Machinery.....	9
RFID Solution Overview.....	9
Step 1 – Tag Printing / Encoding	10
Step 2 – Embedding / Programming the Reader.....	10
Step 3 – Updating Deployed Readers	11
Example 2: Medical Devices	12
RFID Solution Overview.....	12
Product Authentication Using SkyeTek RFID Solutions.....	15
Find out More.....	16
About SkyeTek, Inc.....	16
Sources.....	17

Introduction

Product authentication is the process of verifying or guaranteeing that a product or its consumable is either genuine or permitted to access a particular application. Product authentication protects against counterfeits, substitutes, and generics (CSG) and also provides the manufacturer with additional control over the customer experience ensuring that it meets or exceeds expectations. In addition to being a proven, cost-effective technology, Radio Frequency Identification (RFID) presents the most robust solution for product authentication in the marketplace today.

Historically, product manufacturers have invested in watermarks, holograms, registration schemes, proprietary connectors, and branding to separate their products from CSGs. However, these measures are easily duplicated and oftentimes cost prohibitive. RFID allows manufactures to embed inconspicuous tags, typically costing USD \$0.10 - \$0.30 each, directly into or onto their product or consumable. Once the tag is added to a product or consumable, it can then be encoded with a “digital fingerprint” using state-of-the-art cryptography that uniquely identifies the product or consumable from a CSG. With recent economies of scale and breakthroughs in security, RFID presents the most adaptable and robust answer to CSGs.

The Counterfeiting Epidemic

Counterfeiting is big business. In 2000, trade in counterfeit goods reached an estimated \$450 billion – larger than the GDP of all but 11 countries and about the same size as the total GDP of Australia¹.

Counterfeiting afflicts numerous items across an unthinkable number of businesses:

- Chemical Reagents
- Device Consumables
- Game Tokens / Chips
- Paper Documents / Certificates
- Removable Media
- Replaceable Parts

Consider the economic toll counterfeiting has taken on the following industries:

- 2% of Canon products, film and industrial ink, are counterfeited².
- The world's eight largest Printer companies lost \$2 Billion in 2002 to counterfeits³.
- Counterfeit drugs are predicted to present a \$68 Billion annual problem by 2009⁴.
- The US Institute of Medicine estimates preventable medical errors cost \$17 billion annually⁵. Part of this is due to improper device operation.
- In 2005, 10% of all hi-tech goods (computers, cell phones, etc) sold were fake and accounted for \$100 billion⁶.

Consumables

- Tokens
- Filters
- Tickets
- Contrast Media
- Fluids
- Ink
- Media
- Solution
- Specialized ingredients
- Reagents
- Film
- Toner/Drums
- Award cards

¹ Global Counterfeiting Background Document. APCO, 2003.

² Canon Website, Canon 2004.

³ *Beware Bogus Printer Ink*. PC World, 2003.

⁴ *RFID in Healthcare in 2005*. IdTechEx, 2005

⁵ *RFID in Healthcare in 2005*. IdTechEx, 2005

- In 2005 counterfeit media claimed \$3.8 Billion in counterfeit movie media⁷ and \$3 billion in Video Game media⁸.
- For industrial devices, approximately \$1.8 Billion of counterfeited small arms are traded annually⁹ and an estimated \$2 Billion counterfeited airplane parts are in circulation¹⁰.

Some counterfeited products actually originate from licensed outsourced manufacturers. The third-party factory may manufacture additional units, without the brand owners' knowledge, to then sell the overflow on the black market. This undermines the efforts of some foreign outsourcing brand managers who naively believe that they have impressively reduced their own costs through cheap outsourcing arrangements, only to discover themselves competing against their own brand. In this case, the products behave identically, however, the brand owner is shouldered with support and warranty costs.

Beyond Counterfeiting: Generics and Substitutes

Counterfeiting, however, is only part of the picture. In most cases, manufacturers lose orders of magnitude more business to generics and substitutes. The advent of outsourcing, automation and other technologies have pushed manufacturers to differentiate less on price and more on benefits such as brand and experience. A manufacturer's ability to meet the quality and performance requirements of its customers separates it from the competition and ultimately secures a sustainable competitive advantage.

- **Generics** – Legal emulations, often sold without manufacturer's consent in direct competition. Low cost, low quality generics threaten to deteriorate brand and displace revenue.
- **Substitutes** – Competitive products with minimal switching costs. Substitutes minimize customer lock-in and often undermine a higher quality product.

The Toll of Counterfeits, Substitutes, and Generics

The damage caused by CSGs is substantial and affects most aspects of any product-related business. The pain inflicted by CSGs includes:

- **Lost Revenue:** Revenue gets diverted for both the original equipment manufacturer as well as designers who rely solely on complimentary consumables for profitability.
- **Tarnished Brand Name:** Poor performance can adversely affect an unwitting customer's opinion and experience with the brand. The customer does not blame the poorly performing generic. Rather, he or she transfers the discontent to the original branded product – consequently unwinding years of goodwill and relationship investment.
- **Increased Cost:** Quality and service are sacrificed in favor of price. Poor quality transfers the cost of support and warranties on to the manufacturer, even if they are not responsible.

⁶ *Managing the Risks of Counterfeiting in the Information Technology Industry*. KPMG, 2005

⁷ *The Cost of Movie Piracy*. MPAA and L.E.K., 2006

⁸ *Anti-Piracy FAQ*. Electronic Software Association, 2005

⁹ *Russia to crack down on unlicensed arms production abroad*. Russian News & Information Agency, 2006

¹⁰ *Lasershot Makes Its Mark*. Science & Technology Review, 2001.

- **Threatened Customer Safety:** In environments such as medical devices, industrial filtration and even auto parts, improperly functioning or untested substitutes can lead to consumer injury, litigation and possibly death.

The Benefits of RFID-Based Product Authentication

State-of-the-art product authentication using RFID counteracts the damage inflicted by CSGs and results in the following direct benefits:

- **Revenue Preservation:** Only sanctioned consumables are permitted for use in a product, thus securing a recurring revenue stream for the company or its certified partners.
- **Brand Protection / Customer Loyalty:** Poor customer experiences due to the use of CSGs are minimized. Customer satisfaction levels can remain high reinforcing customer loyalty.
- **Decreased Costs:** Uniform brand quality translates into lower warranty and support costs for the manufacturer.
- **Product Safety:** Minimizes quality risks and flaws and insures that the product is operated in its intended manner – safely and securely.

In addition to direct benefits of product authentication, RFID also offers the following indirect benefits.

- **Customer Visibility:** RFID increases visibility into customer preferences allowing better decisions to be made about product offerings and pricing.
- **Personalized Customer Experience:** Since RFID can uniquely identify people and products, OEMs can use this data to personalize the customer experience with any RFID-enabled product.
- **Correct Product Usage:** RFID allows OEMs to enforce usage policies to ensure correct product usage leading to better quality, higher performance, and more satisfied customers.

How RFID Works

RFID is technology that creates a wireless communication link between a reader and tag (a.k.a. a transponder) using a standard protocol. Though one technology, RFID represents a broad suite of protocols spanning 125 kHz on the low end to 2.45 GHz on the high end.

At a high level, there are two types of protocols, active and passive. Active RFID tags possess their own power source that make them capable of longer read ranges but increase their cost dramatically. An active RFID solution is justifiable in situations where high value items must be identified and tracked over medium to long distances such as a container in a shipyard. Passive tags, on the other hand, do not have their own power source instead drawing power from the electro-magnetic (EM) field generated by the reader. This approach lowers tag costs by orders of magnitude but also lowers read range. Since the vast majority of product authentication use cases require low tag costs and shorter read ranges, only passive RFID protocols in the HF and UHF bands will be discussed in this document. *Table 1* lists common passive RFID protocols in these bands.

Band	Frequency	Common Protocols	High-Level Specifications	Typical Applications
High Frequency (HF)	13.56 MHz	ISO 15693 ISO 14443-A ISO 14443-B	Range: 1 – 15 cm # Tags in Field: 1 – 3 Tag Memory: up to 32 Kbits Tag Cost: \$0.15 – \$3.00 Reader Cost: \$5* – \$500 <i>* requires board level integration</i>	Product Authentication Access Control Patron Management
		ISO 18000-3 Mode 1 ISO 18000-3 Mode 2	Range: 1 – 30 cm # Tags in Field: 1 – 300 Tag Memory: up to 10 Kbits Tag Cost: \$0.15 – \$1.00 Reader Cost: \$200 – \$4,000	Asset Tracking Item-Level Inventory
Ultra High Frequency (UHF)	860 – 960 MHz	EPC Class 1 Gen 1 EPC Class 1 Gen 2 ISO 18000-6A ISO 18000-6B ISO 18000-6C	Range: 0.5 – 10 m # Tags in Field: 1 – 300 Tag Memory: 64 – 512 bits Tag Cost: \$0.10 – \$0.20 Reader Cost: \$200 – \$5,000	Asset Tracking Item-Level Inventory Product Authentication

Table 1 - Common Passive RFID Protocols & Specifications

In passive RFID, each tag has an antenna, analog front end, and digital section allowing it to receive / send RF signals, draw power from the EM field, convert between analog and digital, and apply simple policies based on data received from the reader. Whether or not a tag can apply policies depends on processing capability and memory size of the tag in question.

The RFID reader (a.k.a. interrogator) shares functional similarities to the tag because it also has an antenna, analog front end, and digital section to transmit / receive RF signals, convert between analog and digital, process bits to form an identifier, and apply policies based on the digital identifier. The reader has several traits, however,

that distinguish it from the tag such as a power source, larger size, greater processing power, more memory, connectivity to a host and more programmatic control. When a passive RFID tag is placed on a physical object, the RFID reader that comes across the object in its read field does the following:

- Energizes the tag
- Establishes a connection with the tag using one of the protocols it supports
- Obtains the tag's ID (eg, a 96-bit identifier) and any other data that might be stored in the tag's memory such as date of manufacture, place of manufacture, lot number, date of last service, usage counter, and usage limit
- Converts the analog data received from the tag to digital data that is processed on the reader
- A typical reader in today's RFID market will pass the raw digital data directly to the host application without logic or policy having been applied
- An intelligent RFID reader will apply locally cached business logic and policies based on the data it receives from the tag and may initiate a subsequent transaction such as incrementing the tag's usage counter

As EPC Class 1 Gen 2 tags emerge with extended memory capable of supporting security features such as encryption and anti-cloning, UHF will become an increasingly viable choice for product authentication. When these tags become more broadly available, this white paper will be updated to reflect UHF's position in RFID's portfolio of product authentication solutions and which use cases specifically stand to benefit most from UHF's unique value add.

Picking the Right RFID Solution for Product Authentication

There are two dominant product authentication use cases – Low Volume- and High-Volume-Item Product Authentication – that dictate which RFID protocol is most applicable. The general requirements for each use case are listed in Table 2. Once the use case has been determined, one can quickly determine which specific RFID protocol to use.

Use Case	Low-Volume Product Authentication (LVPA)	High-Volume Product Authentication (HVPA)
Simultaneous Tags in Read Field	1 – 10	10 – 300
Read Range	1 – 10 cm	10 – 100 cm
Read Time	< 1 sec	1 – 3 sec
Reader Type	<ul style="list-style-type: none"> • Reader module embedded in devices / machines • Handheld reader 	<ul style="list-style-type: none"> • Finished reader mounted on or underneath a table or shelf • Tunnel reader
Applicable RFID Protocols	<ul style="list-style-type: none"> • ISO 15693 (longer range, lower data rate) • ISO 14443-A/B (shorter range, higher data rate) 	<ul style="list-style-type: none"> • ISO 18000-3 Mode 2 •
Example Applications (Reader / Tag)	<ul style="list-style-type: none"> • Turnstile / Ticket • Water Fountain / Filter • Gaming Console / Media 	<ul style="list-style-type: none"> • Card Table / Poker Chips • File Cabinet / Legal Documents • Handheld / Medicine Tote

Table 2 – Product Authentication Use Cases

The majority of product authentication use cases today involve Low-Volume Product Authentication (LVPA), so the remainder of this white paper will focus its efforts in that area. As described in Table 2, LVPA is a close-range, few tags-at-a-time use case

that requiring an embedded reader that goes inside a device or a handheld reader that attaches to a device. In either case, users should look for the following attributes in selecting their reader and tag:

RFID Reader

- Small footprint, inexpensive, and low power
- Support for ISO 15693, 14443-A, or 14443-B protocols
- Broad tag interoperability to allow the optimal tag to be selected for the application
- Ability to set policies and application logic on the reader so as to minimize the effect on application performance / code complexity
- Support for proprietary tag security (i.e., CryptoRF from Atmel or Mifare from Phillips/NXP)
- Support for open standards-based encryption and anti-cloning such as Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA), respectively, that provide the following:
 - Modern digital security proven in other industries such as defense, finance, and IT
 - Lower TCO by de-coupling security from tag selection allowing the optimal choice to be made among a broad range of tags
- Application programming interface (API) that does the following:
 - Allows an RFID and / or security novice to quickly and easily direct reader / tag interaction
 - Protects the application from future changes to the underlying RFID protocol and / or tag
- Ability to field upgrade the reader to support new features / functionality in the future

RFID Tag

- Proprietary security implemented directly by the tag and/or,
- Extended memory as required to support open standards encryption / anti-cloning delivered by the reader and to store data required by the application

Example 1: Equipment and Machinery

Equipment manufacturers build their reputations on being able to deliver reliable, high performance machinery that meet or exceed their functional specifications and expected lifetimes. At some point in its life, virtually every machine wears out a part and requires a replacement or uses up all of a consumable and requires replenishment. The manufacturer, type, and age of a part or consumable oftentimes can affect the reliability, performance, and effective lifetime of a particular machine. Any degradation in these parameters, moreover, is likely to negatively affect the manufacturer's brand equity and customer loyalty.

RFID Solution Overview

RFID can be used to solve many of the product authentication issues that equipment manufacturers face. *Figure 1* shows an example of RFID used to authenticate a filter used in an industrial water analyzer. This analyzer is used to assess the suitability of water for specific uses such as drinking, cleaning, or manufacturing. It uses a disposable filter to assist in measuring the levels of certain microscopic particles in water. Filters wear out over time and must be replaced regularly to ensure test result accuracy.

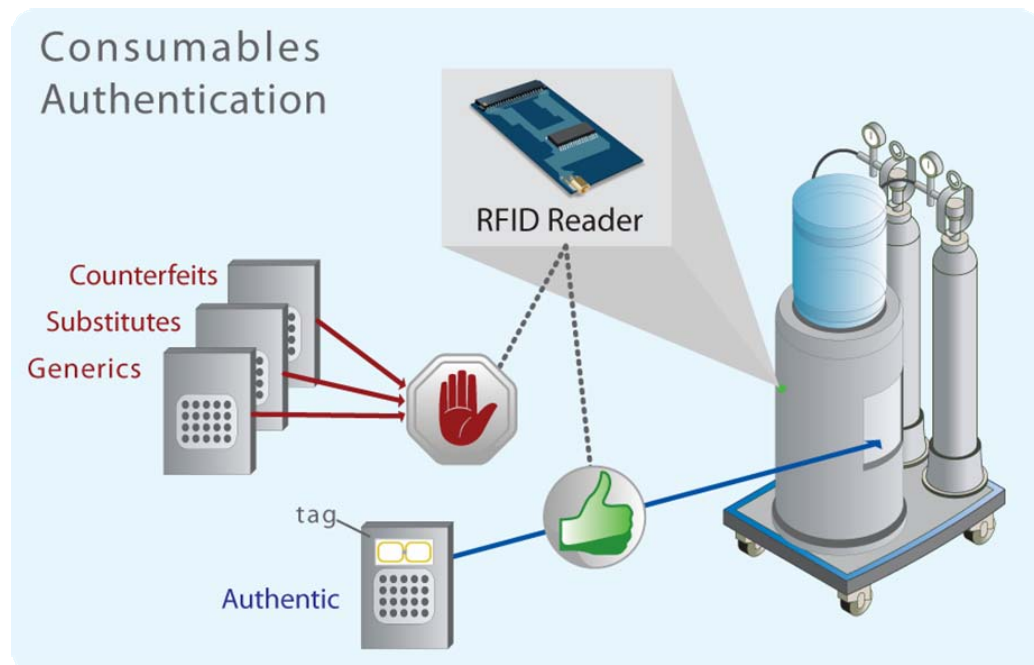


Figure 1 – Product Authentication in a Water Filtration System

RFID is an ideal solution for ensuring that the right filter gets inserted into the analyzer and that the filter is used properly. More specifically, the RFID solution must authenticate the filter's identity and freshness and subsequently authorize its use in such a way as to optimize test result accuracy. A 13.56 MHz HF solution, using either ISO 15693 or ISO 14443-A/B air-interface protocols, is an excellent fit for this use case as it requires a small, inexpensive reader that can easily be embedded into an existing water analyzer and is capable of reading a tagged filter a few inches away. Generic HF tags (i.e., those without proprietary encryption) typically cost \$0.15 - \$1.00 depending on antenna and memory size and come in numerous sizes, from the size of a rice grain to that of a large envelope label. Tags supporting proprietary security protocols are generally more expensive and most HF tags in general are typically 2 – 3 times more expensive than their UHF counterparts; however, HF readers are typically 2 – 3 times less expensive than their UHF counterparts. In this example, the water

analyzer will use less than 300 filters over its lifetime, so the economics favor an HF solution.

There are three steps involved in implementing this RFID solution:

1. Encode the RFID tag with the data required for authentication / usage and attach it to the filter
2. Embed the RFID reader module inside the water analyzer and program it to authenticate and authorize tagged filters that it encounters
3. Update deployed RFID readers in the field with new policies and/or reader features as necessary (eg, to support a different tag in the future)

Step 1 – Tag Printing / Encoding

Completion of this step requires the selection of RFID tags with enough memory to store required identification and policy data and an HF RFID printer / encoder capable of being programmed to encode the RFID tags with usage policies (ie, in addition to identification data for which RFID printers are designed). For example, Zebra Technology's R110Xi-HF RFID printer / encoder utilizes a SkyeTek M2 SkyeModule as its integrated reader engine, so it is capable of encoding tags with this policy information.

As the RFID label is printing, the reader module in the printer encodes the label with data that indicates the filter manufacturer, filter type, date of manufacture, and usage limit. The label is placed on the filter case and shipped to a distributor that keeps an inventory of filters on hand for quick shipment. When a customer orders and receives a filter, the RFID reader module, which has been embedded in the water analyzer authenticates the filter and authorizes its proper use.

Step 2 – Embedding / Programming the Reader

The ideal solution involves using a RFID reader specifically designed to be embedded in existing devices. Primary features for consideration include small size, low power consumption, and standard host interfaces (ie, USB, serial UART, SPI, and I2C) to make hardware integration straightforward.

Likewise, a high-level, intuitive application programming interface (API) that abstracts the underlying RFID hardware and protocols into generic function calls and parameters greatly simplifies integration with host firmware and software. Such an API should be easily understood by RFID novices. As the portions of the underlying RFID hardware change for technical or business reasons, moreover, the common, high-level API insulates firmware and software to which it is tied from those changes protecting the significant time invested in the integration effort.

Once the reader has been embedded in the water analyzer, it is pre-programmed at the factory to only accept filters that meet the following criteria:

- Acceptable manufacturer name
- Acceptable filter type
- Acceptable age since date of manufacture
- Usage below the usage limit indicated on the tag (ie, this policy assumes that the reader keeps track of the number of times a specific filter has been used and compares this count to the usage limit on the tag prior to each use)

As the embedded reader in the water analyzer encounters filters, it will accept or deny filters based on the policies above. After date-specific or usage-specific limits have

been reached, the reader will alert the water analyzer so that it can in turn alert the technician that a new filter is required.

Step 3 – Updating Deployed Readers

Over time, the manufacturer may develop more durable filters that have longer shelf lives. In this case, water analyzers already deployed in the field would need the policies on their readers updated so that they recognized these new filters and used them accordingly.

This can be done either locally or remotely. The new policy can be loaded on physical media and delivered to water analyzer owners for local download to the analyzer (eg, via USB or a serial port). Once downloaded, the analyzer could then re-flash the reader with the new firmware and the policy would take effect once the reader rebooted. If the water analyzer has a network connection, the new policy could simply be downloaded from a host and loaded on the reader. Again, the policy would take effect once the reader was rebooted.

Example 2: Medical Devices

Medical device manufacturers build their brand reputations on being able to deliver accurate test results and proper medication to patients. Achieving this level of trust with patients and practitioners is a difficult task that is made even more difficult by manual errors in equipment usage and generics / counterfeits that degrade device accuracy.

For example, blood transfusions remain driven by manual processes despite significant advances in medical science over the last century. With over 50M blood units transfused annually worldwide, human error in blood type matching will place hundreds of lives at risk every year. Similarly, the accuracy of laboratory test results used in the reagent trail are put at risk by the use of generic or counterfeit reagents used in laboratory analysis equipment.

RFID Solution Overview

RFID can be used to solve many of the product authentication issues that medical device manufacturers face. *Figure 2* shows RFID used to authenticate a chemical reagent used in a urinalysis system. ISO 15693 or ISO14443-A/B is an excellent RFID protocol for product authentication because the tags and readers are small and inexpensive. Moreover, there is a large selection of tag types with different memory sizes for storing data required for the authentication process.

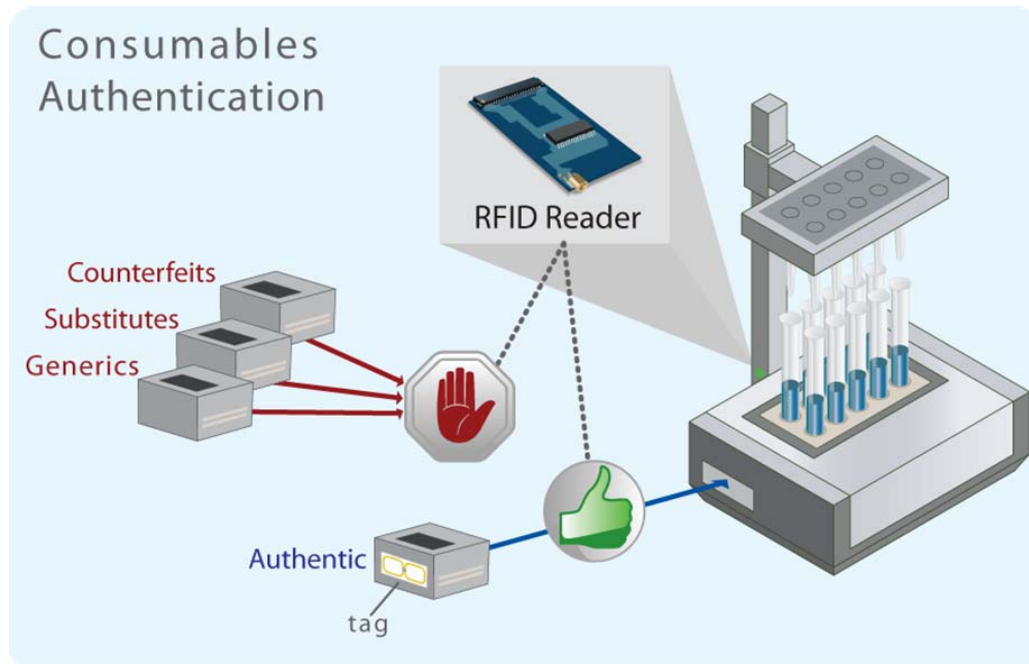


Figure 2 – Product Authentication in a Urinalysis System

The urinalysis system in *Figure 2*, similar to the water analyzer in *Figure 1*, is conducting authentication on the reagent manufacturer / type and authorization on the proper use of the reagent. The difference in this example, however, is that the urinalysis system manufacturer allows third parties to manufacture reagents that can be used with its system. The key stipulation in this arrangement is conformance to published reagent specifications so that test accuracy is not degraded. Certain generic and counterfeit reagents, however, have entered the market and do not meet these required specifications. These unauthorized reagents are materially degrading test results, endangering patient treatment, and affecting the manufacturer's reputation

with its customers. Consequently, the manufacturer would like to immediately execute the following steps:

- Add anti-cloning as part of its reagent authentication process to identify counterfeits
- Create new authorization policies that disallow out-of-spec generics from being used with the system
- Encrypt data placed on reagent tags for added security
- Remotely upgrade RFID reader modules inside urinalysis systems deployed in the field and RFID label printer/encoders deployed in the factory

If counterfeiting is a threat, then open standard cryptography running on the reader is crucial because a generic RFID tag is incapable of defending against counterfeiting. If a numbering scheme or file containing serial numbers is stolen, a counterfeiter can use that information to create counterfeit RFID tags. When placed on counterfeit reagent systems, the RFID reader in the urinalysis system in this example would not be able to distinguish between the authentic and counterfeit reagent.

An RFID reader with open standard encryption and hashing algorithms, such as the Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA), respectively, provides the necessary security to protect against a cloned RFID tag. *Figure 3* shows the same urinalysis system as the one in *Figure 2* but with this additional security. In addition to encoding the data mentioned above on the RFID label, the reader in the printer / encoder would also do the following:

1. Generate a random number (RN) using a pseudo-random number generator (eg, SHAPRNG1) to be used in generating a derived key (DK)
2. Input the Master Key (MK) and RN into SHA hashing function (eg, SHA-256) to generate DK
3. Input DK, the tag's universal ID (UID), and tag data into SHA hashing function to create a "Digital Fingerprint", or keyed-hash message authentication code (HMAC), that uniquely identifies the specific tag and its consumable
4. Encrypt the data and HMAC using AES and the DK
5. Encode the tag with the RN, which is unencrypted, and encrypted contents (ie, data and HMAC)

The reader in the urinalysis system is programmed with the same AES and SHA functions and MK as the printer so that it can authenticate reagent systems that it encounters by doing the following:

1. Read the UID, RN, and encrypted contents on tag
2. Generate DK using MK, RN, and SHA hashing function
3. Decrypt tag contents (ie, data and HMAC) using DK and AES
4. Generate an HMAC using DK, UID, and decrypted data
5. Compare the HMAC generated by the urinalysis system with decrypted HMAC coming from the tag – if the "Digital Fingerprints", or HMACs, match, then the reagent's authenticity has been confirmed
6. The urinalysis system can proceed in using the reagent system based on policies stored on the tag and/or the urinalysis system

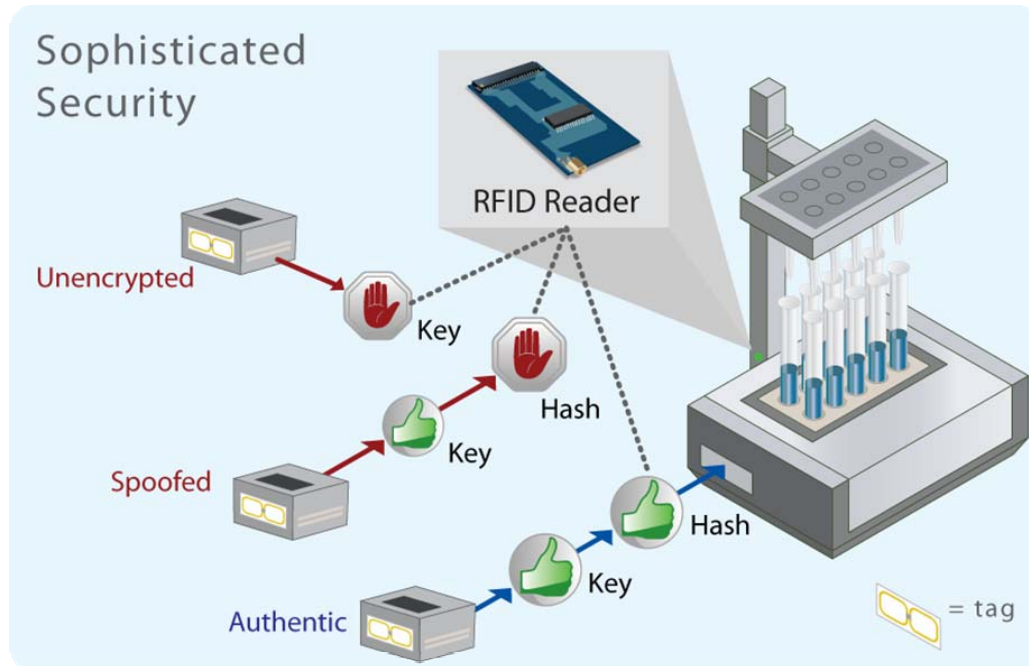


Figure 3 - Product Authentication in a Urinalysis System with Security

The benefit of using open standards encryption and hashing such as AES and SHA are the following:

- a. The AES and SHA families of algorithms have been approved by the Department of Defense and the Federal Information Processing Standards. Both families are made public because of their robustness – it would take a hacker using equipment available today over one hundred years to break these algorithms.
- b. In addition to government-related applications, AES and SHA are commonly used in financial and information technology applications. For example, AES is the basis for WPA-2 which is the industry standard for encryption in WiFi (802.11).
- c. Using an open standards approach to security significantly decreases overall total cost of ownership (TCO). Using open standards security like AES and SHA, the generic tag can be used providing the customer with an inexpensive solution that is robust and field-upgradeable in the event that algorithms and keys are to be changed in the future.

Product Authentication Using SkyeTek RFID Solutions

SkyeTek develops the RFID industry's most cost- / space- / power-efficient readers and intelligent, easy-to-use reader software. In many cases, the RFID reader, which can measure the size of a US quarter, fits unobtrusively into an existing product without requiring any design rework. Coupled with modern, robust security, SkyeTek offers the most advanced product authentication solutions in the world.

SkyeTek reader module benefits:

- Small footprint, inexpensive cost, and low power consumption
- Support for the following passive RFID protocols:
 - HF: ISO 15693, 14443-A / B
 - UHF: EPC Class 1 Gen 1 / Gen 2, ISO 18000-6B / C
- Tagnostic® interoperability to allow the optimal tag to be selected for the application
- Industry standard connectivity: USB, serial UART, SPI, I2C

SkyeTek ReaderWare software benefits:

- Ability to set policies, parameters, and application logic on the reader so as to minimize the effect on application performance / code complexity
- Support for leading proprietary encryption schemes such as Mifare and CryptoRF as well as future algorithms via an on-board 7816 slot
- Industry-leading, open standards-based encryption and anti-cloning such as Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA), respectively, that provide the following:
 - Modern digital security proven in other industries such as defense, finance, and IT
 - Lower TCO by allowing the optimal choice to be made among a broad range of generic tags
- RFID made simple with an API that does the following:
 - Allows an RFID and/or security novice to quickly and easily direct reader / tag interaction
 - Protects the application from future changes to the underlying RFID protocol and/or tag
- Ability to field upgrade the reader to support new features / functionality in the future

SkyeTek works with the world's largest manufacturers and designers to directly embed RFID into their existing and new product lines. Backed by some of the RFID industry's most experienced RF and software engineers and a rich ecosystem of partners, SkyeTek's technology provides a practical, robust solution for product authentication allowing OEM's to secure their product's revenue stream, authenticity and brand equity.

Find out More

Visit www.skyetek.com/fightphonies/ to access a library of valuable resources to assist in evaluating embedded RFID for product authentication:

Case Study: *Iris Diagnostics* – Locks their media for urinalysis machines

Case Study: *Medica* – Protects consumable media in their blood gas analyzers

Case Study: *TioMed* – Automates and controls blood transfusions for increased safety

Case Study: *Water Analysis Manufacturer* – Secures water treatment filters

About SkyeTek, Inc.

SkyeTek develops reader technology and software services that allow customers to embed RFID as a feature into their existing product lines – enabling security, safety, productivity, loyalty and competitive differentiation. Espousing open standards and architecture SkyeTek makes RFID easy to acquire, integrate, secure, connect and utilize. SkyeTek's exclusive focus on embedded technology for OEMs eliminates lock-in and protects investment.

Our sales executives and engineering experts are working with the world's largest product Manufacturers. Contact us today to discover how we can help you preserve your revenue streams and protect your brand by embedding RFID into your existing product lines.

SkyeTek Global Headquarters

11030 Circle Point Road
Suite 300
Westminster, CO 80020

720-565-0441 phone
720-565-8989 fax

SkyeTek EMEA Sales Office

+31-6-2110-7501 phone
+1-303-482-1382 virtual phone

Sources

APCO, *Global Counterfeiting Background Document*, January 27, 2003.

Cannon, Website, Retrieved: 3/21/2007. URL: http://www.canon-europe.com/About_Us/About_Canon/045_Counterfeit/

Tom Spring, *Beware Bogus Printer Ink*, PC World, Retrieved: 3/21/2007. URL: <http://pcworld.about.com/news/Aug282003id112201.htm>

IDTechEx, *RFID in Healthcare in 2005*. Jan 2, 2005. URL: <http://www.idtechex.com/products/en/articles/00000125.asp>

KPMG, Report - *Managing the Risks of Counterfeiting in the Information Technology Industry*, 2005

MPAA and L.E.K., *The Cost of Movie Piracy*. May 2006, URL: <http://www.mppaa.org/researchStatistics.asp>

Electronic Software Association, *Anti-Piracy FAQ*. URL: http://www.theesa.com/ip/anti_piracy_faq.php

RIA Novosti, *Russia set to crack down on unlicensed arms production abroad*. Russian News and Information Agency, December 5, 2006. URL: <http://en.rian.ru/russia/20061205/56488783.html>

Ann Parker, *Lasershot Makes Its Mark*, Science & Technology Review, Lawrence Livermore National Laboratory, September 2001, URL: <http://www.llnl.gov/str/September01/Hackel.html>

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

SkyeTek, ReaderWare and Tagnostic, are trademarks of SkyeTek, Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. SkyeTek, Inc. disclaims proprietary interest in the marks and names of others.

©Copyright 2007 SkyeTek Inc. All rights reserved. Reproduction in any manner whatsoever without the express written permission of SkyeTek, Inc is strictly forbidden. For more information, contact SkyeTek.

Information in this document is subject to change without notice.