Using RFID Technology to Stop Counterfeiting

By Eustace Asanghanwa, Crypto & RF Memory Applications

Summary

RFID technology is well known for providing labeling solutions to automate inventory control. It is less known for its capability to offer anti-counterfeiting solutions. While providing cryptographic authentication schemes with data protection capabilities, a well implemented RFID security solution provides complete product protection against illegal cloning, intellectual property theft, and denial-of-service attacks.
# Table of Contents

*Using RFID Technology to Stop Counterfeiting* ........................................ 1

*Introduction*................................................................................................ 3

*Understanding the Problem of Counterfeit* ............................................. 3

*RFID and Product Labeling*...................................................................... 3

*Assuring Product Authenticity with RFID* .............................................. 4
  - Password Protection ................................................................................... 5
  - Encrypted Labels ....................................................................................... 5
  - Challenge-Response Protection .................................................................. 5
  - Double Challenge-Response Protection ..................................................... 5

*Adding Optional Security for Data Protection* ........................................ 6
  - Write Protection ......................................................................................... 6
  - Data Encryption ......................................................................................... 6
  - Message Authentication Codes ................................................................. 7

*Choosing the Proper RFID Security Solution* ......................................... 7

*Conclusion* ................................................................................................ 7
Introduction

Many people understand RFID as a next-generation barcode with technology to automate inventory control. Few people understand this technology can also protect against counterfeiting and even fewer have knowledge of how or what to consider when shopping for the right anti-counterfeit solution. This paper provides insights to the problem of counterfeiting, how RFID technology can combat it, considerations for a complete RFID security solution, and what to look for when shopping for the right anti-counterfeiting RFID solution.

Understanding the Problem of Counterfeit

Counterfeiting entails illegal cloning of products with the sole intent of deriving economic benefit. The overriding incentive for counterfeiting is easy money without the associated intellectual property and product development costs, quality and reliability concerns. Product manufacturers pay dearly for counterfeiting including brand erosion, loss of market share, intellectual property value dilution, customer support for non-authentic products, and bad will.

Classic solutions to counterfeiting have been tamper resistant/evident packaging, and special label markings. High value consumables like pharmaceuticals, electronics, accessories and cosmetics in today's markets provide incentive for counterfeiters to make capital investments for reproduction of packages and labels to enable cloning. Once they manufacture the appropriate packages and/or labels, they apply them to cheap imitations of the product and go to market. Because the counterfeiter has not incurred the costs typically associated with product development, they quickly cover their capital investments at the expense of the authentic product manufacturer. Counterfeiters have the motivation to surmount any packaging and labeling barriers and often achieve product cloning quite easily. This is because all of the information required for authentication is physically present with the product. Today's products require more advanced solutions to combat product counterfeiting. Effective solutions will require products to carry only part of the authentication information. The manufacturer can keep the other part and so controls production of the product. Holding back a piece of product authentication information as an anti-counterfeit solution works best when dealing with labels. RFID secure labeling provides this capability and requires proper implementation for effectiveness.

RFID and Product Labeling

RFID provides labeling technology like barcodes but with greater capability. Barcodes encode product-labeling information like names and serial numbers but nothing more. They require direct line-of-sight for access, can store only small amounts of information, and have minimum size requirements for effectiveness. As such, small sized items present challenges for item level barcode labeling. RFID technology, on the other hand, embeds labeling information in non-volatile memory devices, which in turn embeds in a product. Unlike barcodes, RFID tags come in various sizes sometimes as small as a grain of rice, have greater storage capacity, and do not require direct line-of-sight for access. The absence of size and line-of-sight limitations allows RFID tags to embed virtually into
any product for flexible labeling down to the item level. This capability enables automatic tracking and inventory control with strategically placed interrogators.

**Assuring Product Authenticity with RFID**

RFID labeling with proper security measures can assure product authenticity and prevent illegal cloning. The necessary precondition for the effectiveness of this scheme is for the product to withhold information until after assuring the authenticity of the interrogator. To achieve this, the tag must expect the interrogator to provide information proving its authenticity. This piece of information is one that only an authentic manufacturer can provide. The tag thus issues cryptographic challenges to the interrogator and will not give out labeling information unless the interrogator provides the proper response. This challenge-response scheme, illustrated in Figure 1, constitutes the proper RFID labeling security necessary to combat cloning. Since the interrogator initiates communications in most RFID protocols, the tag will need to have the challenge always ready. The interrogator would read the challenge and generate a response for the tag to validate. The tag updates its challenge upon a successful response. Counterfeiters, not possessing the proper response to the challenge, will never obtain the labeling information from the device and thus have nothing to duplicate. For example, a shoe manufacturer like Nike may choose to protect its brand and products from piracy using RFID technology. If they embed authentication tags within the shoes, then distributors willing to build a reputation around distributing authentic products can obtain proper interrogator devices from the shoe manufacturer and consumers can feel confident they are purchasing authentic products. High end shoe manufacturers may also find interest in equipping major shopping centers with public authentication checking devices (interrogators) for consumers to validate purchases from hawkers. In either of these cases, pirated products will not pass the validation tests.

Unfortunately, many existing RFID security solutions do not possess this challenge-response scheme thus lacking the infrastructure to protect against counterfeiting. The next few paragraphs highlight some existing solutions and their adequacy.

**Figure 1.** Challenge Response Sequence: Tag Updates Challenge after Every Successful Challenge Response.
Password Protection

Widely used protection scheme but unfortunately the weakest. All it takes is the breach of a single password to retrieve a tag label for duplication. Some tags may implement rolling-password schemes that enhance sophistication but the fact of the matter is that it remains a password protection scheme. It only takes a single password compromise to completely expose the product for illegal cloning.

Encrypted Labels

Some manufacturers go through the pains of encrypting the labels using very strong cryptographic algorithms. They may choose to store these labels in tags possessing password security already for added protection. Unfortunately, counterfeiters do not need to decrypt or understand the labels in order to duplicate them. This protection scheme remains as trivial as that offered by password protection.

Challenge-Response Protection

This scheme requires that tags authenticate interrogators before divulging information. The tags issue interrogators cryptographic challenges for which only interrogators possessing certain secret information are able to respond correctly. By managing interrogator side secrets, authentic manufacturers will possess the ability to prevent counterfeiters from reading their product information thus preventing illegal cloning of their product.

Double Challenge-Response Protection

Similar to the challenge-response scheme with additional ability for the interrogator to also challenge the tag as illustrated in Figure 2. This scheme requires both interrogators and tags to independently store asymmetric secrets to use in the process. This mutual authentication scheme provides assurance to both authentic interrogator and tag about each other’s authenticity. This is particularly useful where authentic interrogators need to provide field updates to authentic tags. For example, interrogators in a mobile electronic application, like smart phone firmware upgrade equipment at a supplier location may need to ascertain the authenticity of the tag (product) before issuing a firmware upgrade. This mutual authentication scheme provides for very powerful counterfeit protection.
Adding Optional Security for Data Protection

The challenge-response and double challenge-response RFID security schemes provide effective anti-counterfeiting solutions. These solutions by themselves, however, do not offer data protection for data communication between the interrogator and the tag. An eavesdropper, for instance, can wait until completion of the challenge-response process and intercept information between interrogator and tag. Depending on the application, they may even modify the information to suite their needs. For example, a malevolent eavesdropper with a competing product can intentionally inject errors in a firmware upgrade to a competitor’s consumer electronic product to achieve a classic denial-of-service attack. Such eavesdroppers may also inject false information into the competitor’s authentic consumables, be it electronic or not, to make them appear non-authentic. A more complete solution to RFID label security thus requires data protection in addition to authentication for most applications. The following paragraphs outline useful data protection schemes with standalone adequacy or in combination depending on the application.

Write Protection

Offered by tags with the ability to lock the data contained within to prevent future modification. This is well suited for pure labeling applications with static label information. Write protection alone may be adequate for the protection of products like pharmaceuticals and consumables including cosmetics, accessories, and apparels.

Data Encryption

Offered by tags with the ability to encrypt information traffic between the interrogator and the tag. Encrypting data between the interrogator and tag assures the confidentiality of the data in transmission. Data confidentially may be useful both in protecting secrets or preventing man-in-the-middle attacks. This protection scheme will be useful in applications where field upgrades are necessary.
Message Authentication Codes

Message authentication codes (MAC) are cryptographic digests that allow the recipient of information to ascertain the authenticity of the source and integrity of the data content. MAC generation uses cryptographic secrets stored within the interrogator and tag. For any given message, only an authentic interrogator or tag can issue the proper MAC. The sender of data thus generates a MAC to accompany the data. The recipient of the data verifies the MAC. If the MAC does not checkout, it either implies that the source of the message is not authentic, the integrity of the message is questionable (i.e. message has been modified since it left the source), or there were channel communication errors. The combination of data encryption and use of MAC provides powerful data protection to field updates like firmware upgrades to electronic products.

Choosing the Proper RFID Security Solution

Many RFID tags offer some level of security but choosing the proper security for your application is the only way to protect your product. The proper security for anti-counterfeiting, at the minimum, requires the RFID tag to possess the ability to authenticate the interrogator prior to divulging labeling information. This provides the authentic product manufacturer control over tag label access by controlling cryptographic secrets needed by interrogators. This prevents counterfeiters from accessing product labels within the tags. There are two things to consider when shopping for an RFID anti-counterfeiting solution:

1. Ensure the RFID tag offers authentication capability prior to access of label information stored within the tag. Look for the challenge-response scheme in applications where the interrogators only need to identify the tag. Look for the double challenge-response scheme (mutual authentication) in applications where interrogators may also need to modify information stored within the tag or product. For example, have interrogators perform mutual authentication with the tags embedded within a consumer electronic device before issuing a firmware upgrade to the product.

2. Ensure the RFID tag offers adequate data protection capability for your application. Look for tags with write protection for applications that require labeling information remain fixed and where the labeling information does not need to be confidential. Look for tags with data encryption and MAC capability for applications requiring assurance of data confidentiality and integrity, and source authenticity. An example of such an application is issuance of firmware upgrades to consumer electronics where the authenticity of the electronic product needs ascertaining, and also where the firmware intellectual property and integrity need protection.

Conclusion

RFID technology can stop product counterfeiting. Combating product counterfeiting requires a paradigm shift from embedding product authentication information within the product to having the authentic manufacturer withhold and control a piece of that information. RFID provides the necessary technology, to include single and double challenge-response authentication security schemes. A complete RFID product protection solution needs to also consider data protection. Data protection schemes include write-
protection, data encryption, and use of Message Authentication Codes (MAC). Depending on the application, a combination of the right authentication and data protection security schemes can provide complete product protection.
Editor's Notes About Atmel Corporation

Founded in 1984, Atmel Corporation is headquartered in San Jose, California with manufacturing facilities in North America and Europe. Atmel designs, manufactures and markets worldwide, advanced logic, mixed-signal, nonvolatile memory and RF semiconductors. Atmel is also a leading provider of system-level integration semiconductor solutions using CMOS, BiCMOS, SiGe, and high-voltage BCDMOS process technologies.

Further information can be obtained from Atmel’s Web site at www.atmel.com.

Contact: Eustace Asanghanwa, Crypto & RF Memory Applications, Colorado Springs, Colorado, USA, Tel: (719) 540-6689, e-mail: easanghanwa@cso.atmel.com