June 2005
White Paper – P01

Securing the Pharmaceutical Supply Chain – The Authenticated RFID Platform

Dr. Andrew D. Dubner, Senior Specialist, Design for Six Sigma Black Belt
3M Security Systems Division

Counterfeiting of Pharmaceuticals

Ensuring a safe and secure pharmaceutical supply chain is an important and challenging task. The need to build security into pharmaceutical products, packaging and supply chains has never been greater because of the increasing sophistication of well-funded counterfeiters. Counterfeiters find pharmaceuticals attractive targets because they are valuable, small, and easy to introduce into the complex supply chain.

The motivation for counterfeiting pharmaceuticals ranges from financial to malevolence. In all cases, these counterfeit products have the potential to cause harm and damage reputations. Counterfeit drugs come in many varieties. There are fake products that have no active pharmaceutical ingredient, products that have been diluted and accurate knock-offs or copycats that have not been approved by the FDA. There are products that have been relabeled in order to misrepresent the potency, expiration date or contents. There are products that have been intentionally or unintentionally contaminated. Finally, there are genuine products that have been diverted from their intended supply chain.

Implementing a coherent security strategy can reduce opportunities for counterfeiting and tampering. This paper describes how a matched component Authenticated RFID Platform delivers a more secure pharmaceutical supply chain. The requirements of a security solution for pharmaceutical products are described. A confidence rating scale is introduced and the platform is described and evaluated in these terms. Finally, the attributes of the Authenticated RFID Platform are discussed in the context of other security features.

Requirements of a Security Solution

The goal of any security system is to ensure that the end product – the product itself – is genuine. However, in the near-term, it is unrealistic to imagine that supply chain participants will be able to directly authenticate the contents of a pharmaceutical product. Thus, the FDA Counterfeit Drug Task Force recommended “a combination of rapidly improving ‘track and trace’ technologies and product authentication technologies” to protect the pharmaceutical drug supply (Combating Counterfeit Drugs, Feb 18, 2004). This approach is aimed at elevating all participants’ confidence that the pharmaceutical product is genuine by addressing three independent components of the product’s life cycle:

1. Authentic packaging – what indications are there that the packaging and associated labeling are genuine?
2. Package integrity – what indications are there that the packaging and associated labeling have not been tampered?
3. Supply Chain history – what information is available to determine that the product has been handled by trusted supply chain partners?

In addition to addressing these components, any practical solution must drive towards automated verification of all security layers without interrupting workflow within the supply chain. Only an integrated systems solution approach can meet these requirements.

Confidence Rating Scale

The confidence rating scale takes the components of a security solution described above and rates them on a four level scale. A more detailed description of the scales is provided in Appendix 1. In general, a rating of zero (Ø) indicates that there is no particular feature or information available to verify. A rating of C, B, or A represents increasing confidence due to the presence of a stronger security feature. An "A" is typically a two-factor approach that integrates electronic and physical security. Figure 1 shows an example of the confidence rating scale in the context of pharmaceutical products.

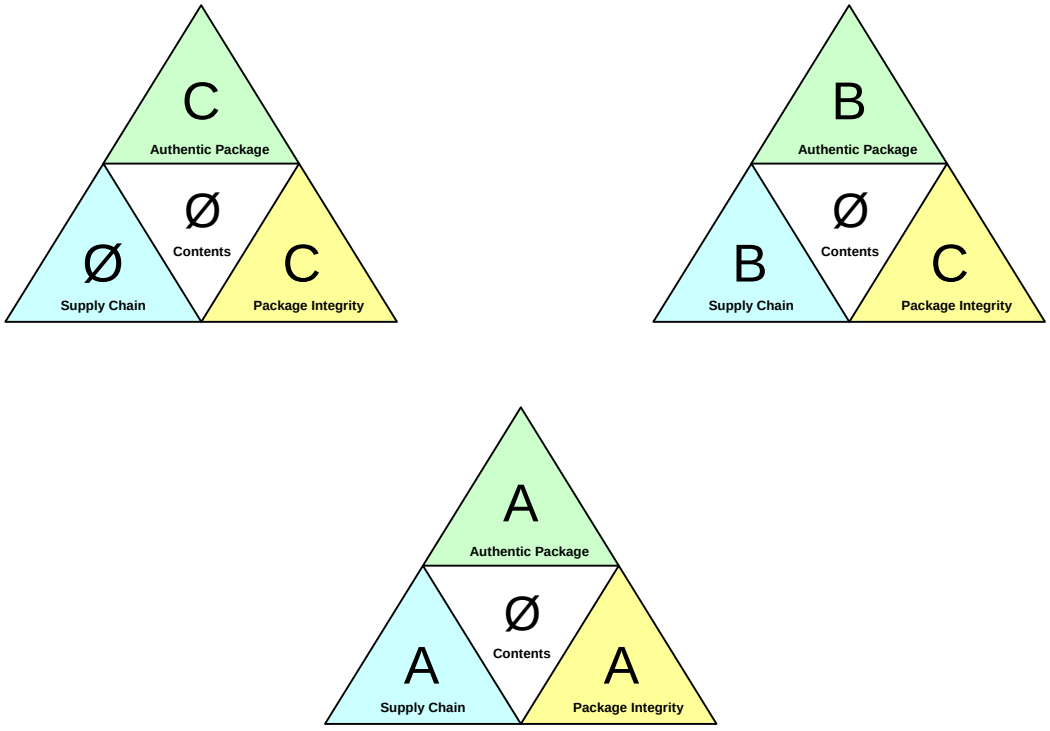

Figure 1 – An example of the confidence rating for typical pharmaceutical product today (top left) indicating the presence of relatively low-level authentication and tamper indication features. The Authenticated RFID Platform will improve the ratings as indicated by the confidence rating at the top right (see description in next sections). In the future, the Authenticated RFID Platform has the potential to dramatically improve the confidence that the pharmaceutical product is genuine as indicated by the confidence rating at the bottom.

Deliverables of the Authenticated RFID Platform

In its most basic form, the Authenticated RFID Platform delivers a machine-readable security stamp in the form of an RFID tag. The tag contains a PKI-based digital signature that provides strong evidence that it came from the original manufacturer. The tag can be authenticated by an authentication reader without being connected to the network (periodic network connectivity is required for PKI updates). The reader can add an event marker (date and time stamp) to the tag to indicate that it was read. The tag/reader security system can be used by multiple manufacturers to create their own security stamp (digital signature) simply by using different encryption keys. The basic building blocks of the Authenticated RFID Platform deliver automated authentication without a network connection.

Additional layering of overt and covert physical security features into the Authenticated RFID label delivers several benefits. First, a layered approach to security is more difficult to compromise. Second, the physical security features allow supply chain participants without readers to verify the authenticity of the tag if they chose to do so. Finally, these physical security features deliver a back-up system to authenticate the package.

As the majority of supply chain participants acquire readers and the network infrastructure expands, the Authenticated RFID Platform will deliver access to supply chain history (or chain of custody). Supply chain participants will authenticate the tag (as with the basic system), and will add information to the network keyed off of the unique item-level identifier that is inherent in the tag and the event market written to the tag. A pedigree can be generated from this information on the network. The authentication reader will include evidence of its authenticity with information sent to the network. This feature provides confirmation that a trusted supply chain participant has handled the product.

The Authenticated RFID Platform is scalable to include future enhancements in security. The basic system can be upgraded to integrate electronic and physical security. As technology develops the system will deliver automated verification of (1) package integrity, and (2) all authentication features on the packaging. This integration of electronic and physical security is analogous to the approach being used by border control agencies to authenticate travel documents (such as passports and visas).

Description of the Authenticated RFID Platform

As outlined above, the matched components of an Authenticated RFID tag and reader system creates the foundation of a strong security solution. It provides immediate improvement in authentication of the packaging and provides identification for supply chain history. It is scaleable to accommodate future improvements into the security solution.

Authentic Packaging – The assessment of Authentic Packaging is related to the ability to verify that the security and identification features on the package and associated labeling

are genuine. The Authenticated RFID tag applied to the product packaging provides a security stamp. The digital signature provides strong evidence that the drug manufacturer applied the tag at the time when the product was packaged. Overt and covert physical security features that can be embedded in the RFID label will provide additional confidence. The combined effect is to provide strong authentication that is difficult to duplicate and simulate and has the ability to be verified by all supply chain participants (with or without a reader). The Authenticated RFID system (reader and tag) elevates the confidence rating for Authentic Packaging to a solid "B" due to the strong authentication of the digital signature. Even without a reader, the Authenticated RFID label can elevate the confidence rating for Authentic Packaging to a "B" or a "C" depending on the physical security set used. More integrated systems will couple the physical and electronic security set to elevate confidence to an "A".

Supply Chain History – The assessment of Supply Chain History is related to determining if trusted supply chain partners have handled the product. This assessment of where the product has been and is going is often referred to as "Track and Trace". The Authenticated RFID tag allows time-stamped Event Markers to be stored directly on the tag. The Event Markers are also stored on the network so that electronic Pedigrees (records of Chain of Custody) can be generated. The reader reports to the network that trusted supply chain participants have handled the product. This system elevates the confidence rating for Supply Chain History to at least a "C" and will elevate it to a "B" as the majority of supply chain participants have readers and can add Event Markers.

Package Integrity – The assessment of Package Integrity is related to indications that the packaging and associated labeling are intact and as intended. Tamper-indicating features can be integrated into the product packaging to provide evidence that the product has not been opened and the contents altered. A tamper-indicating feature can be thought of as a one-time authentication device; if it can be removed and replaced with a duplicate or simulation then it is not effective. Typical features may elevate the confidence rating for Package Integrity beyond a "Ø" to a "C" depending on the pharmacist or end-user's attention to the feature when opening the package. More sophisticated approaches to tamper-indication can elevate the rating beyond a "C" by providing automated verification of Package Integrity.

Contents – The assessment of Contents is related to verifying the authenticity of the actual pharmaceutical product and its efficacy. This is possible in a forensic laboratory, but not at the point of dispensing. In the future, systems may be developed that allow some verification of the actual contents and efficacy in the field. However, in the near-term, it is impractical in most situations to expect the contents to be verified by a pharmacist or end-user. Thus, the confidence rating for contents will generally be a "Ø".

In summary, the key to ensuring a safe and secure pharmaceutical supply chain is a coherent security strategy that employs strong security features. The combination of electronic and physical security offered by the Authenticated RFID Platform solution is a significant advance in protecting the drug supply. Its implementation will immediately elevate supply chain participant confidence in the authenticity of the package and the

supply chain. Integration of tamper indication will further elevate confidence that the product itself is genuine.

General Discussion of Physical Security Features and the Authenticated RFID Platform

There are an expanding variety of security features that provide protection against counterfeiting (authentication) and tampering (tamper indicating). Physical authentication features are traditionally classified as overt, covert or forensic. Overt features are ones that can be verified without the use of a tool. Covert features are ones that can be verified in the field by using a handheld (or portable) tool. Forensic features are ones that can be verified only in a laboratory setting (not in the field). Overt and covert features can have various levels of complexity. Covert tools may be high or low cost.

Authentication features are used to elevate confidence that the product is genuine by providing a feature on the packaging that can be verified as genuine. The choice of using an overt or a covert feature depends on the verification strategy that the brand owner is implementing. In both cases, the effectiveness of the feature depends on the ability of the verifier to tell if the feature is genuine. If the person does not know what to do to authenticate the feature, then simulation will be trivial. Training is key to an effective security solution. Some security features are machine-readable and can be verified automatically. Automated verification of security features reduces the training requirements significantly and allows authentication to occur as part of the normal workflow of the product through the supply chain.

> Overt authentication features can be verified by the eye, or another sense like touch. Examples of overt features include holograms, color-shifting inks, and color-shifting films. Overt authentication features are often used when the end user customer is the intended verifier, however, anyone trained on how to verify the feature can be the intended verifier. Overt features are sometimes included on packaging for their visual appeal, to enhance the appearance of the packaging.
>
> Covert authentication features can be verified in the field using a tool. There are a large number of covert features available. An example of a covert feature is one that can be seen with a particular kind of light, like 3M™ Confirm retroreflective material. Covert features require tools and training, and are most often selected when the intended verifier is a trained inspector. Covert features, however, are sometimes selected when the aim is to have end-users verify the feature, generally when the verification tool is relatively inexpensive and can either be included as part of the packaging or widely distributed.
>
> Forensic authentication features also require a tool for verification, but unlike covert features, the verification often takes place in a laboratory environment or requires a sophisticated hand-held tool. Forensic features by their nature preclude verification by end-users, and are most often used in conjunction with covert investigations.

In-product features are used to provide an authentication feature on or in the product itself. They represent a special subset of authentication features. There are a few in-product features available for use in pharmaceutical products. Like covert features, in-product features typically require tools and training, and are most effective when the intended verifier is a trained inspector.

More than one authentication feature may be included in product packaging. This layered approach to authentication allows different constituents to verify different features and presents a larger barrier to counterfeiting.

Tamper indicating features are used to elevate confidence that the product is genuine by providing a feature on the packaging that can, through changes to the feature, identify attempts to open a sealed package. Any attempt to remove, lift or cut the seal results in an immediate and irreversible change to the seal, alerting the end-user to the possibility of tampering. To prevent a tampered package from being re-sealed with a counterfeit seal, tamper indicating features must also be difficult to duplicate (like authentication features). It is useful to consider a tamper-indicating feature to be a one-time authentication feature. The end-user must know what to look for and authenticate that the tamper indicating seal is genuine when opening the package.

The strength of any security feature depends on the barrier it presents to counterfeiting. Defeating a security feature may involve duplicating the feature or creating a simulation that passes as the genuine feature. The effectiveness of a security solution depends on ensuring that the feature is difficult to duplicate and easy to verify as authentic. If the feature is difficult to duplicate, but so difficult to verify that a simple simulation passes as genuine, then the feature will not be an effective deterrent to counterfeiting. Several factors should be considered when evaluating the barrier to duplication: availability of the base materials, cost of equipment to create a duplicate or simulation, availability of knowledge required to create a duplicate or simulation, and the uniqueness of the technology. But, the question "How secure is this feature?" cannot be answered without knowing how the verifier will be trained. Key questions are:

- What does the verifier need to know (and be able to recognize) to distinguish the genuine feature from a potential simulation?
- How difficult is it to communicate the information that the verifier needs to know?
- How difficult is it to create a potential simulation?

The Authenticated RFID Platform provides a pharmacist or other supply chain participant with a machine-readable security feature. This machine verification provides an automated approach to authentication and eliminates the human judgment involved in verification. The digital signature stored in the electronic circuit of the RFID tag provides strong covert, machine-readable authentication. The RFID tag and reader work together to provide a security system that can be used by multiple manufacturers. Each manufacturer has a unique encryption key and creates a unique digital signature that is stored on the RFID tag. The reader can determine if the tag originated with the

manufacturer by using the unique decryption key that matches the manufacturer's key. In addition, the reader can become the tool used to verify other physical security features. This approach to machine reading security features is similar to the approach being used by border control agencies to authenticate travel documents (such as passports and visas). As described in the confidence rating section above, ultimately the system can be designed to detect an inter-related set of electronic and physical security features.

The Authenticated RFID Platform delivers elevated confidence in the security of the pharmaceutical supply chain. It delivers authentication in the short-term and the ability to build an authenticated electronic pedigree as the network infrastructure builds. The scalable platform provides functionality for additional security and the ability to integrate advances in electronic and physical security.

About the Author:
Dr. Andrew D. Dubner is a Senior Specialist and Design for Six Sigma Black Belt with 3M Security Systems Division. He has a strong technical background in materials science and engineering, including expertise with thin film optics, security taggants, and integrated materials detection systems. He is the co-developer of a covert anti-counterfeiting system for the direct marking of branded products. Dr. Dubner holds a Ph.D. in Materials Science and Engineering from the Massachusetts Institute of Technology. He is the co-inventor on five patents, and the author of numerous technical publications.

About Security Systems Division:
For more than 30 years, 3M has provided premier security solutions and services that identify, authenticate, secure and track materials and information by combining security and productivity. Drawing on its broad technology base and expertise, 3M creates solutions for a wide array of security needs. Examples include issuance and authentication of travel documents and personal identification cards, brand and asset protection solutions to fight counterfeiting and tampering, file tracking solutions, and library security and workflow management solutions.

About 3M – A Global, Diversified Technology Company
Every day, 3M people find new ways to make amazing things happen. Wherever they are, whatever they do, the company's customers know they can rely on 3M to help make their lives better. 3M's brands include Scotch, Post-it, Scotchgard, Thinsulate, Scotch-Brite, Filtrete, Command and Vikuiti. Serving customers in more than 200 countries around the world, the company's 67,000 people use their expertise, technologies and global strength to lead in major markets including consumer and office; display and graphics; electronics and telecommunications; safety, security and protection services; health care; industrial and transportation.

3M, Scotch, Post-it, Scotchgard, Thinsulate, Scotch-Brite, Filtrete, Command and Vikuiti are trademarks of 3M.

Appendix 1 - Confidence Rating

The confidence rating system rates four factors: Authentic package, Intact package, Supply Chain history, and Contents. Four ratings are possible: Ø, C, B, A. The following definitions apply:

For Authentic package

- Ø– general knowledge and inspection, no particular feature to verify
- C – low level security feature set, ranges from one that can be easily replicated or simulated to one that takes some minimal effort to defeat
- B – high level security feature set, this typically involves a security technology that includes
    - A single (or restricted) source of material
    - Very high cost to replicate – equipment and/or knowledge
    - Unique technology – difficult to simulate
- A – independent high-level electronic and physical factors that are inter-related through a system that uses the electronic factor to prescribe the physical factor(s).

For Intact package (same rating scale as Authentic package)

- Ø– general knowledge and inspection, no particular feature to verify
- C – low level security feature set, ranges from one that can be easily replicated or simulated to one that takes some minimal effort to defeat
- B – high level security feature set, this typically involves a security technology that includes
    - A single (or restricted) source of material
    - Very high cost to replicate – equipment and/or knowledge
    - Unique technology – difficult to simulate
- A – independent high-level electronic and physical factors that are inter-related through a system that uses the electronic factor to prescribe the physical factor(s).

For Supply Chain history

- Ø – general knowledge, no particular information that validates history
- C – direct knowledge of product origin
- B – direct knowledge of product origin and pedigree that represents a reasonable path through the supply chain
- A – direct knowledge of product origin and pedigree with risk profile accepted by expert system

For Contents (verified at the point of dispensing)

- Ø – general knowledge, no particular feature in or on the product to verify
- C – low level security feature set or indicator in or on the product, ranges from one that can be easily replicated or simulated to one that takes some minimal effort to defeat
- B – high level security feature set or indicator in or on the product
- A - independent high-level electronic and physical factors that are inter-related through a system that uses the electronic factor to prescribe the physical factor(s).