Supply Chain Security and Loss Prevention Through Effective Counterfeit Prevention and Detection RFID Data Structure

AVANTE International Technology, Inc.
70 Washington Road, Princeton Junction, NJ 08550
www.avantetech.com

INTRODUCTION

In the year 2000, the World Health Organization estimated that more than 7% of the world's pharmaceuticals were counterfeit. In the United States alone, the loss to counterfeit drugs was estimated to be in the range of $2 billion. By 2005, the estimate of the world's pharmaceutical supply chain loss was more than 10% of the world supply of drugs or US$32 billion a year❶.

Concerning the less mission critical supply chain arena, the financial loss to counterfeit commodity products amounted to more than $500 billion and more than 7% of all trade in 2004 ❷. The loss was high enough that the Federal government started a federal program called "Strategy Targeting Organized Piracy (STOP!) ❸" to stop the epidemic.

It is well known that barcode technology cannot prevent counterfeiting since they can be easily duplicated, made up, and "copied". It is less known that unless radio frequency identification tags or labels are properly made to protect against counterfeiting, they may have similar vulnerability as lesser cost barcode technology.

The current international RFID usage protocols such as those in EPC and ISO standards 18000 and 15693 are deficient in handling the possibility of products labeled such RFID tags being counterfeited❹❺.

AVANTE pioneered the development of RFID tags for counterfeit drug prevention using a patented end-to-end tracking and tracing process for pharmaceutical supply chain visibility❻. In a 2001 white paper, AVANTE put forth that "RFID chip has a unique serial number that cannot be duplicated. In addition, HIPA-TAG uses a patent-pending "relational-check-code" method to encode on the read-write" memory segment and to read and authenticate the data encoded on the tag as demonstrated on the far right of the (figure 3) in form of warning manifest."❼

In preventing counterfeit, RFID has the potential to be an extremely cost effective tool when properly harnessed. It must be protected from unauthorized changing or tampering of data encoded used to identify a product. It must also be inherently impossible to be duplicated.

In the application of pedigree management of medical drugs, ideally, we can write onto the tag the date-time at each of the distribution points. Because of the requirement of ISO and EPC standards must be "universal" to allow everyone to read all tags, the traditional encryption techniques cannot be used to protect the data on the tags after they have been encoded. Alternative method must be devised to help authenticate the data that was written onto such tags.

NOT ALL RFID TAGS CAN BE USE TO DEFEAT COUNTERFEITING

In order to fully appreciate the difficulties in defeating counterfeits of RFID tagged products, one must understand the difference between various international standards and some of their deficiencies. Table 1 is a list of various data formats used for EPC class 0, 1, and 2. Similar deficiency is carried through to class 3, 4, and 5. In fact, the deficiency is so obvious that a simple device can be used to defeat the system through simple swapping of the codes on tags already placed on the products❽. The same means and techniques can be used by organized efforts in producing counterfeit products.

The ISO 15693 and ISO 18000 series of standards on RFID are more secured against counterfeiting. They have the on-tag factory hard-coding “permanent code”. The inclusion of this “permanent code” provides the possibility of faster detection of counterfeits.

Table 1: Comparative Analysis on Security of RFID Data Formats, Protocols, and Standards Against Counterfeiting

RFID Data Format	Benefits & Deficiencies	Counterfeit Prevention Capability
Write-once only serial number	▪ Automatic identification. ▪ Must link to the database-of-origin to know what is in the tagged box. ▪ Error may occur in reading the code without noticed.	▪ No. Even if the database of origin can be accessed, there is no way to authenticate direct copy of serial numbers that are constructed or “copied” from the database of origin. ▪ No if system is not online. ▪ No if database-of-origin is not accessible.
Write-once only serial number + Application specific data	▪ Automatic identification. ▪ More application data even if database-of-origin is not accessible. ▪ Error may occur in reading the code without noticed.	▪ No. Even if the database of origin can be accessed, there is no way to authenticate direct copy of serial numbers that are constructed or “copied” from the database of origin. ▪ No if system is not online. ▪ No if database-of-origin is not accessible.
Write-once only serial number + Application specific data + on tag CRC (Current EPC code)	▪ Automatic identification. ▪ More application data even if database of origin is not accessible. ▪ Reading error is minimized or eliminated. ▪ EPC compliant.	▪ No. Even if the database of origin can be accessed, there is no way to authenticate direct copy of serial numbers that are constructed or “copied” from the database of origin. ▪ No if system is not online. ▪ No if the database of origin cannot be accessed.
Permanent number Only	▪ Automatic identification. ▪ Must linked to the database-of-origin to know what is in the tagged box ▪ Error may occur in reading the code without being noticed.	▪ Yes if the database of origin can be accessed. ▪ No if system is not online. ▪ No if the database-of-origin is not accessible.
Permanent number + Applicable data	▪ Automatic identification. ▪ More application data even if database of origin is not accessible. ▪ Error may occur in reading the code without noticed.	▪ Yes if the database of origin can be accessed. ▪ No. No way to know if the application data has been “changed” or “tampered” with if the system is not online or database of origin is not accessible.
Permanent number + Applicable data + On-tag CRC + On-tag additional Relational-Check-Code on top of on-tag CRC	▪ Automatic identification. ▪ More application data. even if database of origin is not accessible. ▪ Reading error is minimized or eliminated. ▪ Tampered data can be discovered. ▪ ISO 18000 compliant.	▪ Yes if the database of origin can be accessed. ▪ Yes even if the application data has been “changed” or “tampered with” even if the system is not online. ▪ Yes even if the database-of-origin is not accessible, the “relational-check-code” will found the changes.

EPC DATA SCHEME AND THEIR VULNERABILITIES

Figure 1 below is a representation of the current EPC coding scheme:

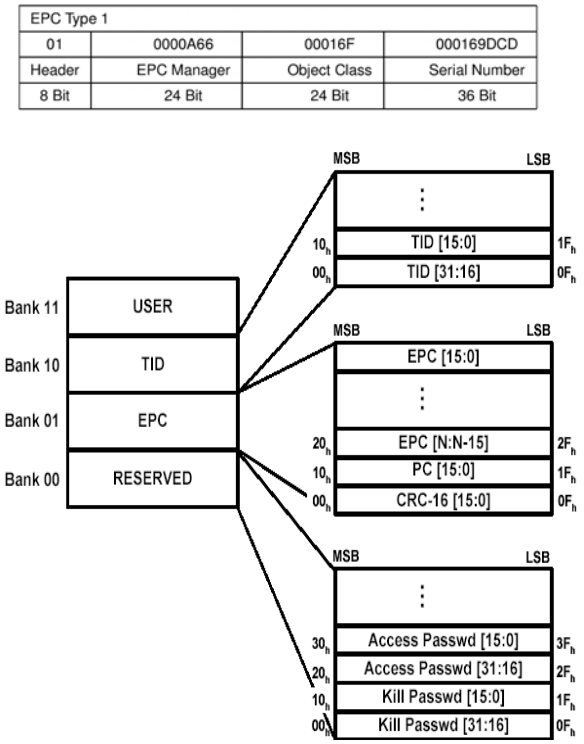

Figure 1: The number or coding scheme adopted for the current class 1 Generation 2 UHF passive tag. A 16-bit CRC on-tag relational-check-code is added to help the accurate data deciphering even in a heavily used and interfered environments.

A 16-bit CRC check code is included in the encoded data on tag to ensure correct reading. Instead of using traditional transmission CRC check, it uses on-tag encoded CRC check as prescribed in the AVANTE inventions❾❿. The inclusion of this on-tag CRC check code helps to minimize any errors in heavy interfering environment when many readers and tags are being used at the same time.

While the use of standard CRC check code ensures ease of use and open architecture of the system, it also provides no protection against tampering of any data that has been originally written onto the tag. The tampering party and system will self-consistently recoded the CRC after data has been modified or tampered with. That is, one can easily change an extremely expensive item to a low cost item code. Many computer experts have pointed out this weakness.

Even more problems relate to the lack of "permanent" or "hard coded" code used to identify individual RFID tag. Instead each EPC tag sold is an empty "white" page that allows any information to be written. This deficiency in design is fatal in the attempt to defeat the counterfeit epidemic. The lack of uniqueness in each tag enables unlimited copying and duplication of tags issued by any manufacturer. The cost barrier is very low and costs only a few hundred dollars to the counterfeiting parties.

ISO 18000 and 15693 DATA SCHEME AND THEIR VULNERABILITIES

Figure 2 below is a representation of the current ISO 15693 and ISO 18000 data coding scheme:

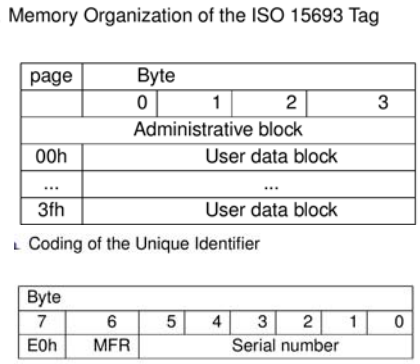

Figure 2: ISO coding scheme includes a "permanent" tag ID but lacks the on-tag CRC code for data validation. In a "heavily" RFID application environment, many data may be read incorrectly. While the usage of "permanent" unique tag ID provides inherent counterfeit detection capability, it must be used in conjunction of network availability and the database-of-origin.

The difference between EPC and ISO coding schemes is the incorporation of a unique factory "hard-coded" tag identifying code. The

missing part is the on-tag CRC or other relational check code. The incorporation of the permanent and unique tag identifier makes simple copying of a valid tag almost impossible and thus has the potential to defeat counterfeit attempts. The only requirement is the availability of the "database-of-origin" so that valid tag ID and the tagged data can be validated. The communication network must also function so that cross-referencing can be made timely and easily in real-time.

The lack of on-tag relational-check-code could be a problem in heavily RFID populated environment. The interference sometimes causes the mis-deciphering of the tag data. The incorrectly read data easily went unnoticed.

The lack of some form of off-line validation protection or tampering detection can present problems where Internet or network availability is a problem. The same problem applies to the situation or condition where the database-of-origin is not available.

Table 2: Vulnerabilities and methods of counterfeiting

1.	EPC "phishing" and mass tag copying	▪ Tag used read/write chip is like a blank piece of paper. ▪ It is relatively straightforward to copy data that is known to exist and produced for products tagged with EPC codes. Basically, anyone buying an EPC reader/writer today can perform such tasks. The costs and barriers for counterfeiting are low. ▪ The valid serialized numbers can be easily obtained or guessed. ▪ An "industry" of EPC code "phishing" may be created for the counterfeiters.
2.	EPC code direct copy	• Even if one provides some means of protecting the valid codes to the "public" one cannot protect against people that can read tags that are on the shelve or somewhere along the supply chain. ▪ Valid serial numbers can be "copied" and copied as many times as the counterfeiters wish to cause more confusion in the supply chain.
3.	ISO 18000 and 15693 and EPC application data may be changed or tampered	• Even though both ISO and EPC protocols allow the "locking" of the encoded data, they are not the required scheme. ▪ If the data is not locked, it can easily be tampered with. A dangerous drug can easily become "aspirin". ▪ Even if the tagged data is locked, new tags can be "copied" and modified as part of the tampering.

SUMMARY OF EPC AND ISO DATA SCHEMES AND VULNERABILITIES

There are several vulnerabilities that must be addressed before an RFID tag coded with electronic data can be secured against counterfeiting and tampering.

To help understand some issues related to deficiencies in current EPC standards in preventing counterfeit products, Table 2 below outlined the various methods where tags and thus tagged products can be counterfeited.

The vulnerabilities can be relatively easily prevented with a simple relational-check-code along with a "hard-coded" tag identification code from the factory. The barrier to counterfeiting chips with factory burn-in codes raises the bar to such a level to make counterfeiting much less attractive to even the most organized efforts.

There is no easy way to fix the counterfeit attacks on the current EPC code scheme. While the more established ISO 15693 standard having a permanent factory burnt-in code is more secure, its effectiveness against counterfeiting relies completely on the availability of the database-of-origin. If the network is not available, the counterfeit products cannot be detected. This could be a problem in time-sensitive point-of-care application in a hospital or clinic. It may present even more problems for those countries that have less established Internet.

Even if Internet accessibility is not a problem, other Internet based vulnerabilities appeared in financial and commercial activities are also shared in the EPC applications. Bogus databases posted by the drug counterfeiters and "phishing" are some of the problems to be addressed by the industry.
Some may also argue that by following the "pedigree" of the products, one may be able to manage the product counterfeit problem.

However, when a counterfeit product has been detected, they may have already passed through several distribution nodes. It may be very difficult to positively identify where counterfeiting occurred. That is, while pedigree can help, it may be costly to find the culprit as to render it ineffective.

More importantly, not ALL counterfeit products can be found before they are used. This could be a huge problem in mission critical pharmaceutical industry.

ADDITIONAL PROTECTION OF EPC DATA CAN BE ADDED WITH MINIMAL COSTS

AVANTE believe that the current EPC code must be modified or add additional categories so that permanent hard coded tag ID is part of the coding scheme like that of the ISO 15693. The addition of the hard-coded permanent ID for each RFID tag raises the bar for any attempt to counterfeit the tags by simple copying. The cost barrier is believed to be high enough to make it unattractive to criminal enterprise.

ISO 15693 should be modified to include a CRC code to ensure that data is read correctly. The addition of CRC or similar check code on tag is particularly important in an environment where multiple readers and multiple tags are being read in nearby locations causing interference and collisions. AVANTE has found the use of relational-check-code to be essential in ensuring error-free reading of tag data. The traditional use of communication based CRC code is not effective in detecting minor bit errors that occur frequently in environments using multiple readers.

Figure 3 below is a coding scheme that AVANTE uses for applications in dealing with the mentioned vulnerabilities. It is relatively easy to add additional check code like that of MD5 type of data binding that is commonly used in preventing changes in electronic data files. Adding this layer of data integrity protection provides two additional benefits that do not impact on the efficiency of reading the tags with the current EPC or ISO protocol.

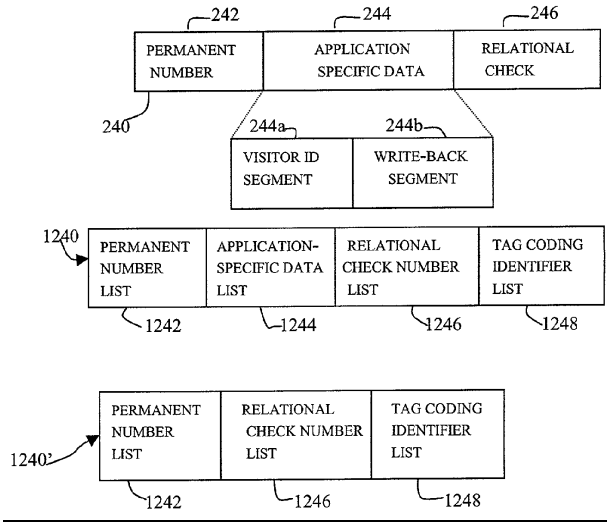

Figure 3: ISO coding scheme includes a "permanent" tag ID but lacks the on-tag CRC code for data validation. AVANTE now patented method binds the "permanent" number and application data into a "relational-check-code" in addition or replacing the CRC code that is stored on the tag memory. Only stations with authorized firmware writing the date-time and ID for the drug pedigree management will be able to re-generate a correct corresponding check code. Standard ISO or EPC readers can read the tags correctly and thus maintain the open architecture. Any data change by readers without proper firmware will be detected. This method serves to authenticate the tag with or without the availability of the more complex future EPC network.

That is, during the sortation or other fast moving operation, only the 96 bits of the EPC data is read. The additional "MD5" type of relational-check-code can be read only during point-of-sales or point-of-care or point-of-dispensing depending on the application. Reading all the data up to 1 k bits, as in the ISO 15693 is still less than 1 second.

The addition and incorporation of another layer of "relational-check-code" to the EPC or ISO coding scheme does not impact the currently designed applications of EPC. In fact, such "relational-check-code" can even be "customized" for a specific industry or manufacturer to provide even higher security.

For example, the pharmaceutical industry can incorporate a industry wide "MD5" like code that can be further customized with a vendor-specific private code for all there products encoded with customized encoders. While the supply chain partners can read the data, their readers will not be able to encode or change the data on the tag without causing an alert of data tampering.

That is, such method provides for a capability of "encrypting the data" without closing the "openness" of the ISO or EPC standards. Additional check-code allows the detection of tampering or counterfeiting even if the Internet or the database-of-origin is not available.

CONCLUSION

RFID has the potential to benefit the supply chain with both improved efficiency and security and end-to-end visibility using a suitable tracking infrastructure.

One of the side benefits is the prevention of counterfeit products. Along with the recovery of financial losses of multi-billions of dollars to the drug manufacturers, in the case of the mission critical products such as pharmaceutical medications and drugs, it also could mean life or death to the patients that require such medications.

The current EPC code does not provide means to identity counterfeit products. With a relatively small adjustment or by adding another class to the current classification with a unique permanent tag identifier for each tag would dramatically enhance the security against tampering and counterfeiting.

An addition of an industry-specific MD5 type encryption-based relational-check-code will provide additional security even without the online connection or availability of database-of-origin. The costs of such minor additions are a fraction of the potential benefits of financial gain or the saving of a human life.

Based on the annual US $500 billion counterfeit losses alone, using RFID tags to uniquely identify each item of value above $50 will pay for itself with abundant returns.

REFERENCES:

❶ FDA, "Combating Counterfeit Drugs Report", February 2004: http://www.fda.gov/oc/initiatives/counterfeit/report0204.html

❷ Frank Giovinazzi, "Federal Gov't Announces New Anti-Piracy Initiative", Oct 7, 2004, AIADA, http://www.aiada.org/article.asp?id=24501
Jonathan Krim, "Anti-Counterfeiting Initiative Launched", Washington Post, Oct 5,2004

❸ US Immigration and Customs Enforcement, "Strategy Targeting Organized Piracy (STOP!), October 4, 2004, http://www.ice.gov/graphics/news/factsheets/STOP_FS100404.htm

❹ George V. Hulme, Thomas Claburn "RFID's Security Challenge" InformationWeek; Nov. 15, 2004 http://www.informationweek.com/story/showArticle.jhtml?articleID=52601030

❺ The Advisory Council, "Smart Advice: Write IT Plan For Nonprofit That Incorporates Values: *Question B*: What security issues do we need to consider in using RFID?" Information Week, October 25, 2004 http://www.ice.gov/graphics/news/factsheets/STOP_FS100404.htm

❻ Kevin Chung, "Medical assistance and tracking system and method employing smart tags", US patent application 10/247,435 (Published 2003/0052788)

❼ Kevin Chung, "Elimination of medication errors through Positive Patient Medication Matching", December 2001 http://www.aitechnology.com/avantetech/Elimination%20of%20medical%20errors.pdf

❽ Lukas Grunwald, "RF-ID Smart-Labels: Myth, Technology, and Attacks", Blackhat Briefings, July 2004 http://www.rf-dump.org/

❾ Kevin Chung, "Article tracking system and method", US patent 6,883,710

❿ Kevin Chung et al., "Smart tag data encoding method", patent allowed US application 10/171,015 (Published 2003/0006878)