Protection against counterfeit medicines by means of digital signatures

Submitted as a contribution in response to the European Commission's public consultation in preparation of a legal proposal to combat counterfeit medicines for human use

by

Isaac Leo Bain
(citizen of Brazil)

08 May 2008

address: Alameda Itu, 890
Sao Paulo, SP 01421-001
Brazil

phone: + 55 11 3082-6165
fax: + 55 11 3082-4245
email: leobain@attglobal.net
email: leobain@duraveis.com.br

Summary

The intent of this work is to submit to the Commission's consideration a technique that can greatly help in combating counterfeit medicines and, by virtue of that, may inform the discussion of the legislative and technical aspects of this project. "Greatly help" means:

- It gives consumers an easy, fast and sure way to check the authenticity of a product
- Its efficiency is independent of the specific technology used to commit information to and retrieve it from packages (linear bar code, data matrix, RFID chip etc.)
- With it, there is no need for "physical" authenticity seals or marks (such as holograms etc.)
- It makes successful combating of counterfeits independent of supply-chain traceability
- As a consequence, it lets countries attain very effective protection of its citizens against counterfeit medicines in the short run

The technique is a variant of mass-serialisation, namely: commit to each package a cryptographic signature (a.k.a. digital signature) of the concatenation of the product's serial number with a short description of it. What follows is a detailed explanation of this.

This technique also makes it effective and inexpensive, independently of the degree of supply-chain traceability, to:

- Combat theft, diversion and contraband of medicines
- Prevent sales of expired products
- Enforce product recalls immediately

Introduction

The World Health Organization's IMPACT report "Anti-counterfeit Technologies for the Protection of Medicines", produced in its general meeting of 12/12/2007 in Lisbon, classifies anti-counterfeit technologies in four groups, according to the type of authenticity mark on the product: overt, covert, forensic and serialisation/track-and-trace. The way IMPACT describes them, in the first three groups the evidence for authenticity comes from an analysis of the physical characteristics of the mark, and in the fourth type from an analysis of the information contained therein. There is an implicit distinction between security supported by form and security supported by information contents.

The technique described here is a hybrid of two of these four groups. It belongs to the last one: security of authenticity supported by the content of information derived from serialisation, namely a digital signature. At the same time, it possesses the essential characteristic of the first group (overt) as defined by the O.M.S.: consumers are able to verify the authenticity of a medicine by themselves.

For the most part, overt technologies are based on adding a "physical" mark to the product – for example, a hologram, a scratch-off patch, luminescent fibers embedded in the package material, a special seal etc. A layperson must be able to recognize it as authentic, but often cannot distinguish between an authentic mark and a reasonably good imitation.

A digital signature, in contrast, is a virtual mark of authenticity that relates directly to the product's description. The consequence of this for the consumer is that it makes possible much easier and unequivocal recognition of authenticity. And for manufacturers it makes possible, at a lower cost, complete control over what can reach consumers, even before full traceability of the supply chain is available. Because it is based on a virtual mark of authenticity, this technique renders impracticable not only counterfeiting, but also theft, diversion and contraband. The table below compares information-based and "physical" authentication schemes.

	Digital signature	Holographic stamp	Scratch-off patch	Packages made from special paper	Special seal
Cost	Small if printed as a simple bar code	Cost of stamp	Cost of patch	Cost of the paper	Cost of seal
Authentication by the consumer	Simple and unequivocal	Simple but difficult to distinguish from the well-made imitation	Consumer has to sratch off	Simple but difficult to distinguish from the well-made imitation	Simple but difficult distinguish from the well-made imitation
Security against fraud	Signatures are inimitable	Reasonable imitation possible	Only works if consumers bother to scratch	Reasonable imitation possible	Reasonable imitation possible
Security against theft	Yes	No	No	No	No
Security against diversion	Yes	No	No	No	No
Consumer checks authen-ticity but decides not to buy	No problem	No problem	Problem	No problem	No problem
Recall	Takes effect immediately	As presently	As presently	As presently	As presently

What are digital signatures

Traditional cryptographic techniques – that is, methods used to cipher and to decipher data or messages – used to have something in common: the same secret (key) used to cipher was also used to decipher.

A mathematical invention of the 1970s opened way for the creation of a new type of cryptography. Called asymmetric cryptography, it is characterized by the following property, surprising at first: the key that is used to decipher is different from the one used to cipher. They form a pair, that is, one only "opens" what the other one "closed," but knowing the first does not allow deducing the second. Therefore only one of them needs to be private, and the other one can be of public knowledge.

Diverse methods of asymmetric cryptography exist, many of them in the public domain (not patented or with expired patents). This type of cryptography has been studied by specialists for decades and is presently considered the most secure there is.

Asymmetric cryptography can be used to prove the origin of a piece of information, and from this to prove the origin of a product. It goes as follows: a pharmaceutical industry (call it the Manufacturer) chooses a private key that it keeps secret, and divulges the corresponding public key for decoding. The Manufacturer puts on the product information encrypted with the secret private key. Preferably this information is something directly related to the product, for example its commercial name and specs. Anyone can decipher that encrypted information with the aid of a machine, since the key to decrypt the information is public knowledge. If the deciphered information makes sense (i.e. if it is the correct name and specs of the product), it means that only the true holder of the private key could have ciphered it. That is, any encrypted piece of information that makes sense when deciphered is a proof of its own origin – in other words, it is a signature of the Manufacturer.

Moreover, this digital signature is inseparable from the information whose origin it is proving. The holder of the private key can use the same key to encrypt different pieces of information (different serial numbers concatenated with different product names and specs etc.). Each piece of information produces a different digital signature. It is impossible to associate a true signature to false information.

To make an analogy with signed papers: it is impossible to take a true signature as model and imitate it on another document. And it is impossible to cut a true signature and paste it onto another document.

For years now, digital signatures have been widely used in many countries to prove the origin of digital information. What is proposed here is that they be used to prove the origin of medicinal products as well. In countries where medicines are sold in their original packages, rather than being dispensed by a pharmacist, this technique enables manufacturers to not only eliminate counterfeiting, but also to put an end to theft and diversion of its products, as explained below. Additionally, should the need to recall certain lots arise, it provides a quick and efficient way to do it.

The proposed technique in detail

In its database, the manufacturer associates a unique serial number with each product unit it sells. That serial number is then concatenated with a short description of the medicine, for instance its commercial name and other specs such as form of presentation, concentration and expiration date. The manufacturer then uses its secret encryption key to generate the digital signature of that concatenated information. It then puts that digital signature on the package, along with a numerical code that identifies the manufacturer. The digital signature is different for each package, but the encryption key is the same.

Each drugstore would have a device called a "checker" that customers can use at will. A checker is, on the outside, a piece of equipment much like the price-checking terminals that exist in many stores and supermarkets, with which consumers can check the price of a product before they decide to buy it. It retrieves information from products and shows short texts on the display. (For the customers' convenience, bigger drugstores may have as many checkers as they would like.)

When the consumer puts the product near the checker, it reads from the package both the numerical code that identifies the manufacturer and the digital signature. From the first, the equipment identifies the appropriate deciphering method to correctly decode the signature. Decoding is then done, and the original information recovered. The checker now looks up in its memory a table of periodically updated data, and verifies whether the unit identified by that serial number is listed there as "authorized" at that moment. If it is, the checker displays the product's name and specs, for example:

COMMERCIAL-NAME 200 mg
30 capsules - exp.: MAY 2012
XYZ Pharma

All this takes just a fraction of a second because all the steps are done off-line (i.e. without those few seconds of waiting that would otherwise be necessary if authentication were done on-line). The consumer sees that what is on the display is exactly what was expected, and so considers the product authentic. If the display showed anything other than the exact description of the medicine the consumer is holding, it would not be the legitimate item.

Since knowledge of the deciphering method gives no knowledge about the encryption method, the deciphering software can reside in the checker's memory without compromising security.

And also, since what goes on the product is not the serial number but rather its digital signature (which no one other than the manufacturer knows how to generate) the list of all “authorized” serial numbers can reside in the checker’s memory as well, without compromising security.

Consequently all the steps just described (deciphering, table look-ups etc.) can be done locally, off-line, so the consumer gets the answer instantly. There is no need for the checker to connect itself with the manufacturer's computer at authentication time, so there is no delay. With this technique, authentication is quick, easy and reliable.

Cashiers' terminals at the drugstores would be programmed to take those same steps when ringing up a medicine. Independently of whether or not the customer had bothered to check authenticity with one of the checker devices, the cashier's terminal automatically retrieves the information from the package, deciphers the digital signature and looks-up its table of authorized units. If it gets a "not authorized" answer, the sale of that product is blocked. Again, everything is instantaneous so the consumer doesn't have to wait.

As soon as the sale of a medicine is registered, the list of “authorized” serial numbers in the memory of all checkers and cashiers’ terminals at that drugstore is updated with the information that the unit just sold will no longer be considered authorized there. I.e. the cancellation of that unit’s "authorized" status takes place only in that particular drugstore's equipments, since at that moment the system is operating off-line. What prevents counterfeiters from re-using or copying discarded packages to try to sell the counterfeit product in other drugstores is that all the other drugstores' checkers and cashiers’ terminals eventually also get the updated list of serial numbers that lost their “authorized” condition.

Periodically, for example once a day, late at night, the computers in the retailers would exchange information with a central database. They would report the serial numbers of the medicines sold at their location during the period, as would all the other drugstores, and then receive from the central database an up-to-date list of all of the authorized serial numbers for the current period. The serial numbers of the sold medicines cease to be authorized everywhere. This system-wide update takes only a few minutes, and after that the system reverts to off-line operation. A one-day window of opportunity is not enough time for counterfeiters to beat the system.

If the original package of a medicine that had already been sold is re-used or duplicated, and someone submits that original or its copy to authentication by a checker, the table look-up will detect that it is not an authorized serial number and the equipment will display a warning message such as "**PRODUCT NOT RECOGNIZED**" – not accusing anyone, but enough to discourage the consumer from buying it. And even if the consumer does not bother to use the checker to verify authenticity, the cashiers' terminal will block the sale.

How to put digital signatures on packages

The security of digital signature-based authentication is indifferent to the vehicle used to add that piece of information to the package – be it a linear bar code, a data matrix, an RFID chip or any other vehicle. Consequently, in order to have anti-counterfeiting capability in place as quickly as possible, the suggestion is that initially the vehicle be a traditional linear bar code to allow for immediate implementation taking advantage all the infrastructure and equipment already in existence to print and capture data. The technology of printing and reading linear bar codes is inexpensive and widely available.

On the other hand, when in a few years pharmaceutical industries decide to migrate to different technologies such as bi-dimensional bar codes or RFID chips, the system migrates smoothly along to any of those technologies, with no discontinuity. The only change necessary would be to upgrade the checkers and cashiers' terminals to be able to read bi-dimensional bar codes or RFIDs. The core of the software would remain the same.

In fact, in the future different countries can come to standardize different ways to add information to a medicine. But as the essence of the anti-counterfeiting technique proposed here is independent of them, its application can accommodate possible geographical differences of technology that may come to exist.

Note on the "initial stages": If linear bar codes are adopted in the initial stage in order to expedite things, the question arises of how many different serial numbers can be represented. The omnipresent bar codes readers of today, even the simplest, are able to read without difficulty codes that represent up to 16 decimal digits. "Without difficulty" means that laypeople are able to obtain a reading in the first attempt.

If the first 3 digits be used to identify the manufacturer, it will be possible to identify a thousand different manufacturers. The remaining 13 digits would be the digital signature. To each serial number corresponds a signature and vice versa, therefore it is possible to identify 10^{13} distinct units of medicine of each manufacturer. Taking into account the number of units currently commercialized by the pharmaceutical industry, and assuming excellent rates of annual growth of sales, 13 digits allows for the univocal identification of each unit to be commercialized by all the manufacturers in next the 20 years or so.

Numerical example: Assuming that each manufacturer commercializes 200 million units this year, and that sales in units grow 30% a year, signatures with 13 digits are enough to individualize all of the units commercialized in next the 35 years.

Security of digital signature-based authentication

Fake packages with “made-up” digital signatures

When checkers and cashiers’ terminals try do decipher the signature, the result makes no sense, so the equipment displays the message “**PRODUCT NOT RECOGNIZED**" – enough to discourage the customer.

Copy or re-use of authentic packages

The serial number is correctly retrieved but, as the equipment checks whether it is authorized, it gets a negative answer and displays the message “**PRODUCT NOT RECOGNIZED**."

Theft and robbery

If products are stolen from stock or cargo is robbed en route, then as soon as the manufacturer gets notice of the occurrence it puts the system on-line with all the computers at the drugstores and cancels the "authorized" status of all the stolen/robbed units. This operation takes only a few minutes, and is done much before the criminals can make the merchandise reach the marketplace.

Diversion and contraband

The system also prevents diversion, including contraband, as follows: there are infinitely many encryption keys to generate digital signatures from. To prevent diversion, it is sufficient that the manufacturer choose different keys for different destinations. The meaning of "destination" is whatever is convenient for the manufacturer: it can be a country, a region, a state etc. If the manufacturer so desires, it can even use a different cryptographic key for each chain of drugstores. If diversion occurs, when the checker or the cashier's terminal tries to decipher the information on the product it will get something that makes no sense, and therefore the unit will not be authenticated and its sale will be blocked.

Alteration of the expiration date

The encrypted information on each package may contain the product’s expiration date. This makes it useless for a counterfeiter to falsify the printed date. As the checker or the cashier’s terminal decodes the information, it detects that the product is past its expiration. The product is not authenticated and its sale is blocked.

Recall

Another benefit that stems from the manufacturer’s complete control over the “authorized” status of each unit produced is the ability to enforce a recall effectively and immediately. If the need for a recall should arise, the manufacturer can at once get on-line with the drugstores and cancel the authorization of the corresponding units. From then on, these units would no longer be authenticated, and their sales would be blocked. Physical retrieval of the suspended products can take place later.

Tracking products

The system lets the manufacturer know exactly which units ended up being sold at which drugstore. Since each unit has its own individual encrypted information on it, and since both the checkers and the cashiers' terminals decode and record every signature submitted to them, the manufacturer has full access to this information, brought up to date daily during the late-night, online system-wide updates.

Communication with the consumer

This authentication system gives the manufacturer a direct communication channel with consumers, at a time when they are paying great attention to the message they are receiving. Besides the name and specifications of the drug, the manufacturer may complement the displayed text with other communication such as the price, a health tip, or an institutional or promotional message such as "**NOW AVAILABLE IN 100 mg CAPLETS**", for example.

Cost sharing

Although up to now we have been talking about a single manufacturer, this anti-counterfeiting system can accommodate a large pool of pharmaceutical companies sharing the same hardware, software and communications infrastructure, with no added costs. This would not compromise security. Each manufacturer would choose its own secret encryption keys, and the secret needs not be shared because what is programmed into the checkers and cashiers' terminals is only the (open) decryption methods. As a consequence, the participating companies can share all set-up costs except for that of putting the signatures on packages.