Anti-Counterfeiting Using Memory Spots

Helen Balinsky, Edward McDonnell, Liqun Chen, and Keith Harrison

Hewlett-Packard Laboratories,
Long Down Avenue,
Stoke Gifford,
Bristol, BS34 8QZ, UK
{helen.balinsky,edward.mcdonnell,liqun.chen,keith.harrison}@hp.com

Abstract. We propose a new hardware and software solution for anti-counterfeiting that puts product authentication directly into the hands of end-users, enabling them to be confident of the authenticity of a product regardless of the integrity of the distribution chain. This is made possible by a new type of tamper-resistant hardware chip, called "memory spot", which has a unique combination of small size, very fast on-air data rate, relatively large memory, and integrated security features, in conjunction with a novel authentication protocol. In addition, the low cost of these new chips makes our proposed solution even more compelling than possible alternatives. Example applications include pharmaceutical anti-counterfeiting, asset tracking, secure-ID, brand protection and warranty fraud prevention. We will take pharmaceutical anti-counterfeiting as an example to explain our solution. A prototype system has been built to demonstrate the feasibility of the proposed system.

Key words: RFID, memory spot, anti-counterfeiting, package authentication

1 Introduction

There is no doubt that counterfeiting of consumer products is a rapidly growing problem; in particular counterfeiting of pharmaceutical products creates enormous health and safety issues as recent examples have demonstrated. The war between counterfeiters and anti-counterfeiting is on-going. Traditional anti-counterfeiting technology includes barcodes, holograms, tags, special printings, etc. According to the accords with the US FDA (Food and Drug Administration) recommendation, there is a unique identification for every unit of packaging [1], [2]. Researchers of information security and cryptography have made use of RFID (Radio-Frequency Identification) in this area, e.g. [3], [4], [5]. A more recently work by Staake et al [6] has proposed building an RFID-based supply chain security system, where each product has an RFID tag, which holds a unique hardware identity number; this number can be traced from supplier, distribution center, and port to consumer. For stronger protection, the RFID tag can also hold a secret key to support cryptographic mechanisms. In order to achieve

security of the supply chain, the RFID tag must have a Physical Unclonable Function (PUF).

Supply chain security using RFID has become well-known and has been considered to be a successful solution for anti-counterfeiting in the research community. However, in real practical applications, a traditional supply chain still dominates the marketplace. This chain includes multiple entities, such as many wholesalers, but only two entities, i.e. the manufacturer and retailer, are visible to a customer (end-user). The secure supply chain requires the involvement of many entities between the manufacturer and retailer. Most likely it would take many years to build such a secure supply chain in practice. Furthermore, in some applications, such as pharmaceutical anti-counterfeiting, revealing and verifying all details of every entity in the supply chain could be difficult and unnecessary, because there may be some requirement on anonymity.

In this paper, we provide two contributions to the anti-counterfeiting research. Our first contribution is use of a new type of tamper-resistant hardware chip, called "memory spot", instead of using ordinary RFID devices. Compared with RFID, the memory spot is much smaller and therefore suits pharmaceutical applications very well. Our second contribution is a simple authentication scheme, called the package authentication scheme. Our goal with this scheme is not to make it a replacement of RFID in supply chain security, but we suggest this scheme could either be used alone before the RFID supply chain security is ready or be used as a supplement for the RFID secure supply chain.

Our proposed hardware and software solution is well suited to the general authentication problem for goods or items that are stored or transferred over potentially non-secure channels [7]. This solution has wide applicability and can be applied to the anti-counterfeiting of pharmaceuticals and other goods, as well as to warranty fraud, asset tracking, secure-ID, brand protection and many others. Such a wide spread of applications is made possible by the unique technical attributes of the memory spots.

We define the authenticity and validity of goods or drugs to mean that they are the products they claim to be (i.e. they match their prescription, description, list of installed parts, etc.), that they are made by the stated manufacturer and that they have not expired. The problem is addressed by providing an end-user product authentication solution, rather than the current process of remote verification through a referential system ([8], [9]).The proposed solution also tackles the grey market problem, where otherwise genuine drugs or goods are resold into a different geography than originally intended.

The proposed solution brings authentication directly to the point of sale. It is a new multi-level authentication scheme that increases the confidence that the consumer or end-user has in the product. Confidence level is extremely important as demonstrated in trials of the solution proposed in [8]. This also makes last minute product recalls not only possible, but extremely easy to achieve. At the time that the customer checks the authenticity of the product, he is connected to an up-to-date website that can also provide the recall information. This avoids the latency problem of the conventional recall distribution chain.

The leading and most advanced area in combating counterfeit goods, the pharmaceutical market, is currently realizing that the best time and place to check whether products are genuine and come from the original manufacturer, is when they are finally delivered to the end-user, regardless of how many times they have changed hands on the way. It was strongly emphasized at the Pan-European Summit for Pharmaceutical Manufacturers [10] and in a report by Forrester [11] that in order to ensure that drugs are safe and efficacious they should be authenticated when pharmacists deliver them to the patient. Our solution is therefore both extremely relevant and timely.

The remainder of the paper is arranged as follows. We will introduce the functionality of memory spots in Section 2, followed by the proposed product authentication scheme in Section 3. In Section 4, we will analyze potential threats and the security of our solution. In Section 5, we will show some brief comparisons between our solution and some already existing solutions, and we will conclude the paper in Section 6 with some comments on future work in this research topic.

2 Overview of Memory Spot Functionality

In our solution, we make use of memory spots [12] as a replacement for RFID devices. A memory spot is a tamper-resistant hardware chip. A micrograph of the memory-spot chip is shown in Figure 1. The unique features of the mem-

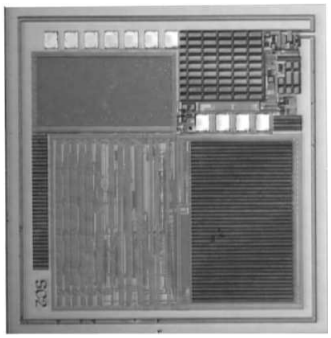

Fig. 1. A micrograph of a memory-spot chip

ory spot are its small size (2 mm^2), its very fast (10 Mb/s) on-air data rate, relatively large memory sizes and its processor. Figure 2 shows the size comparison of the chip alongside pencils and a laboratory prototype of a memory-spot reader/writer.

A memory spot tag deployed for the pharmaceutical anti-counterfeiting solution proposed in this paper holds the following functionalities:

1. It can provide between 32 KB and 512 KB of Write Once Read Many (WORM) type of memory, which is sufficient for high resolution images of

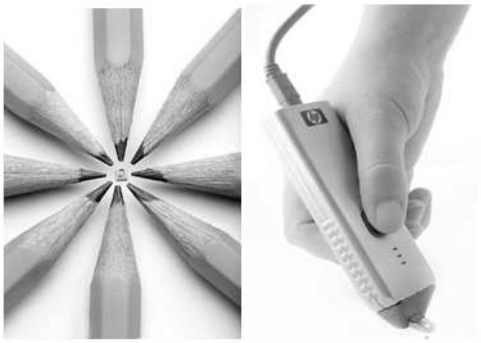

Fig. 2. (left to right) Size comparison of the chip alongside pencils; a laboratory prototype of a memory-spot reader/writer

packaging (a so-called "fingerprint"), together with full product provenance, expiry date, etc.
2. It has a restricted access function to its memory, by which we mean the contents of the memory cannot be read by an unauthorized user, but can be accessed by the on-board challenge-response circuitry (this memory is used for holding a secret shared by a batch of memory spots).
3. It has a unique non-clonable and non-modifiable factory programmed identity ID that is read correctly in a trustworthy manner by a memory spot reader.
4. It is physically very small (2 mm^2 in area and 0.3 mm thick) and can be fitted securely and unobtrusively into something as small as a vial, a blister pack or the seal on top of a bottle of pills.
5. The access range to the memory spot tag is physically restricted to less than 2 mm, so it is reasonably easy to shield the tag to prevent reading or writing until the packaging is actually broken.
6. It has challenge-response circuitry, i.e. it can compute a response to a challenge value by using the stored secret. This function allows the memory spot to play the role of an on-board challenge response authenticator (based on a standard cryptographic primitive) which defends against cloning and impersonation attacks.

Note that a basic solution of this application works even if the memory-spot does not have the functions of restricted access memory and challenge response circuitry. This means that the memory spot is a storage only device with a unique ID, which could also be a cheaper option. However, in that case, memory spot authentication cannot be performed. Therefore, the basic solution might be vulnerable to an impersonation attack that is specified below. In the remaining part of the paper, we do not discuss this basic solution in detail because the assumption of no impersonation attack might be too strong in the real world.

3 The Package Authentication Scheme

As mentioned before, the goal of our package authentication scheme is to provide an authentication mechanism for a traditional supply chain environment, in which there are multiple middle-men but only the manufacturer and retailer are visible to the end-user. Our authentication process is therefore run at the point of final sale for a product. Authentication at the point of sale requires trusted electronic data to be delivered to an end-user simultaneously with the item. This is a considerable challenge. In this section we present the simple and practical package authentication scheme that uses the unique features of the memory spot, as specified in Section 2.

3.1 Design Principles

According to the FDA, for a variety of reasons, counterfeit drugs are currently most likely to be introduced into the distribution chain where there are multiple wholesalers [1], [2], [13]. As we cannot trust the whole chain, we trust:

- The foundry: that they make memory spot chips as specified above and that they do not have leaks of memory spots without preprogrammed ID.
- The pharmaceutical company: that they originate the correct drugs in the correct packaging.
- The actual dispensing pharmacist: that the genuine authentication application is used.

When memory spot readers are ubiquitous the pharmacist can be removed from the list of trusted parties. Before that time they can be replaced by independent authentication kiosks.

There are two distinct parties involved in the authentication process: the manufacturer, for example a pharmaceutical company, and the end-user. By end-user we mean anyone who is authenticating a product. It could be a pharmacist or retailer, either when they receive and authenticate a wholesale package of goods or when they dispense an individual drug to a consumer. It could also be a consumer, who verifies the drug at the point of sale themselves.

The memory spot tags employed by this solution have a physically enforced WORM memory (Write Once, Read Many times) which is only ever written to by the manufacturer and under the same secure conditions as when the drugs or goods are manufactured. After the required data has been written, the write functionality is irreversibly disabled in the hardware so that no new data can be added or the existing data altered. Also, there is some restricted access memory, where the manufacturer can store a secret H, but which can only be accessed for reading by the on-board processor through its challenge-response circuitry.

In the following a couple of subsections, we will describe the actual processes followed by the manufacturer and the end-user with reference to the schematic diagram shown in Figure 3.

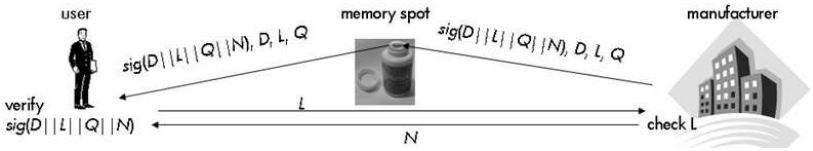

Fig. 3. The Package Authentication Protocol

3.2 Parameters

To simplify further reading in Table 1 we provide a short list of the parameters, which are used in the specification of the proposed package authentication scheme. Anything with a star $*$ is a retrieved version of the original data that has possibly been altered.

3.3 Creation of an Authentic Package

In the process of setup the manufacturer creates a public and private key pair for the purpose of making digital signatures. An authenticated copy of the public key should be made available to the end-user, and the corresponding private key is held securely by the manufacturer. This part can be done by using an ordinary asymmetric cryptographic technique, such as PKI therefore we will not discuss it further.

A flowchart of the manufacturer's procedure of creating an authentic package for each product described below is shown in Figure 4.

During manufacturing a memory spot P is securely attached or embedded in each unit of packaging or item for sale. Each package is assigned two unique random integer numbers. Let us call them login L and nonce N to approximately reflect their roles. A range for both login and nonce should be selected to ensure that there is a sparse distribution of used numbers, so by knowing one or a few numbers it is impossible to infer other logins and nonces. L and N are stored in a secure database owned by the manufacturer, where L is used as a primary key entry for a particular unit or item. The database entry also includes a flag to indicate its status.

Then, a description D of the product is generated. For a medicine it is likely to include product provenance and ID, instructions for use, quantity, dosage, expiry date and actual photographs of the individual item showing all of its particular (customized) features, including the so-called packaging "fingerprint". In the case of a warranty application it might include part descriptions, their unique IDs and respective warranty periods. If the memory spot is embedded or attached to the packaging or product by means of a secure seal, then the seal ID will also be included.

The factory fitted unique identification Q is retrieved from the memory spot P and combined with the description D and login L to form a single message $M = D||L||Q$. This is written to the WORM area of the memory spot. Then, a new message F is formed by appending the previously generated nonce N to

Table 1. A short list of parameters

D	is a description of the product. For a medicine it is likely to include product provenance and ID, instructions for use, quantity, dosage, expiry date and actual photographs of the individual item showing all of its particular (customized) features, including the so-called packaging "fingerprint". In the case of a warranty application it might include part descriptions, their unique IDs and respective warranty periods. If the memory spot is attached to the packaging or product by means of a secure seal, then the seal ID will also be included.
P	is a memory spot.
L	is a login: a unique random integer number that is used as a primary key entry for each unit of packaging in the manufacturer database.
N	is a nonce: a secret random integer number that is recovered from the manufacturer database during a product authentication.
Q	is the factory fitted memory spot unique ID.
M	is a message obtained by concatenation of D, L and $Q : M = D\|\|L\|\|Q$. It is written by the manufacturer to the memory spot P.
F	is a message formed by appending the nonce N to the message $M : F = M\|\|N$. After the digital signature of F is computed this message is discarded.
N^*	is the retrieved nonce.
M^*	is the message that is retrieved by the verifier from the memory spot P. M^* should be equal to M if it is genuine.
F^*	is a reconstructed message formed by appending the retrieved nonce N^* to the message M^* recovered from the spot: $F^* = M^*\|\|N^*$.
R	is the digital signature of the message F that is written by the manufacturer to the memory spot P.
T	is the control spot: a memory spot programmed with a secret that matches the secret H residing within the memory spot P attached to a product.
H	is the manufacturer secret shared by the memory spots P and T.

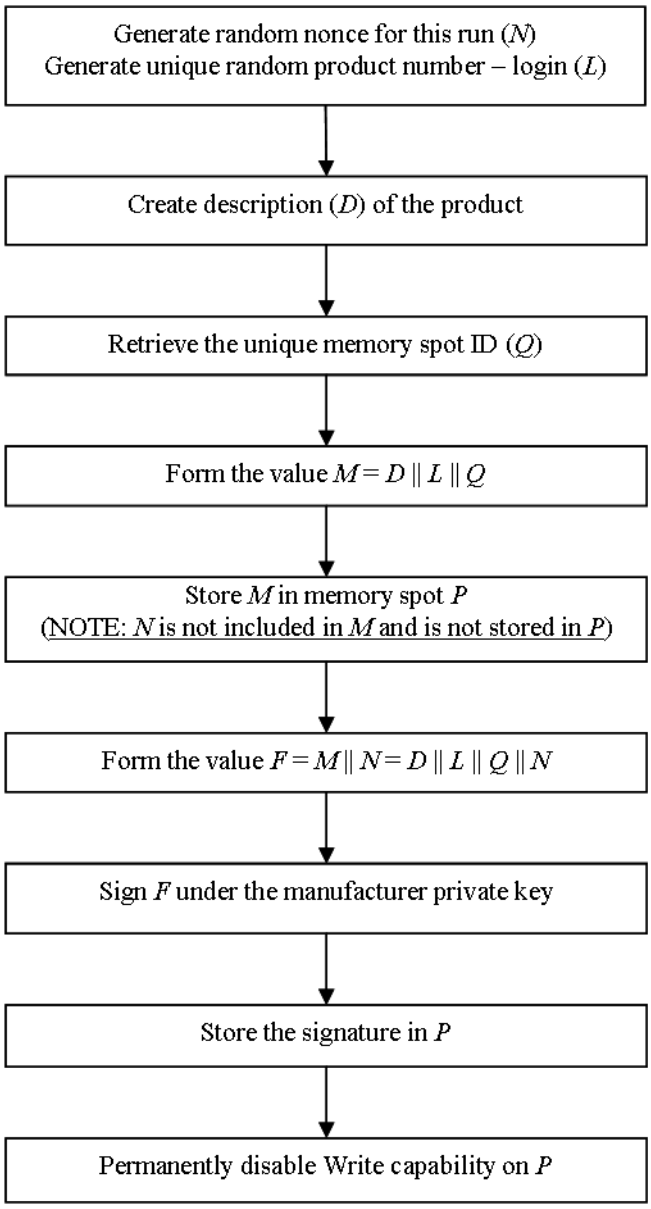

Fig. 4. The manufacturer procedure (issuing the Signature)

the message $M : F = M||N$. The digital signature R of message F is computed using the manufacturer's private key and then stored with M.

Summarizing, all the relevant product information in the form of the message M, as well as the digital signature R, is stored on the memory spot. However, this does not provide sufficient information for signature verification due to the missing value of nonce N. Next, some secret H (previously generated per batch or lot, i.e., the secret is shared amongst a batch of memory spots and the manufacturer) is written into the restricted access memory and finally, the write functionality is disabled and the memory spot shielded from outside access.

3.4 Verification of the Authentic Package

The flowchart of the end-user's verification procedure described below is shown in Figure5.

We assume that the verifier has access to a trusted copy of the manufacturer's public signature verification key and a corresponding "control spot" T from the manufacturer. T is a memory spot programmed with a secret that matches the secret H residing within the memory spot P attached to a product. There should be a clear indication which T should be used for a particular item (package). We also assume that the verifier knows the contact information, such as the IP address or telephone number, to communicate with the manufacturer or other alternative authority.

First, the verifier checks that the packaging is intact and breaks it in order to read the contents of the memory spot P. The verifier loads T into a slot in the memory spot reader and instructs it to challenge P by sending the same random string to both T and P. The digests returned from T and P should match, and if they do, it is safe to assume that the secret in both memory spots is the same and hence the memory spot P must and can only have originated from the same place that issued T, i.e. the manufacturer.

Message M^*, that should be the combination of $D||L||Q$ that was written by the manufacturer, is now retrieved from P. The login L^* is extracted from the message and sent to the manufacturer, who checks whether it is valid. For valid L^* the corresponding flag is subsequently tested, and if it is clear, the manufacturer sends the corresponding nonce to the verifier and then sets the flag. If the flag is not clear, the manufacturer responds to the verifier by either not returning the nonce at all or returning it with warnings - for example "Warning: This drug has already been verified. Is it being resold?" The manufacturer makes a record of every communication.

After receiving N^* the message F^* is formed by adding it to the retrieved message M^*. Now the end-user has sufficient information to verify the digital signature using the manufacturer's public key. The signature R^* is retrieved from the memory spot P and verified. If this fails, then the verifier is alerted, otherwise D^* and Q^* can be trusted. The next step is to compare Q^* with the factory fitted memory spot ID to ensure that the data has not been copied from another memory spot. Finally, the verifier checks that the product matches what is described in D^*, which may include the packaging fingerprint, expiry date and

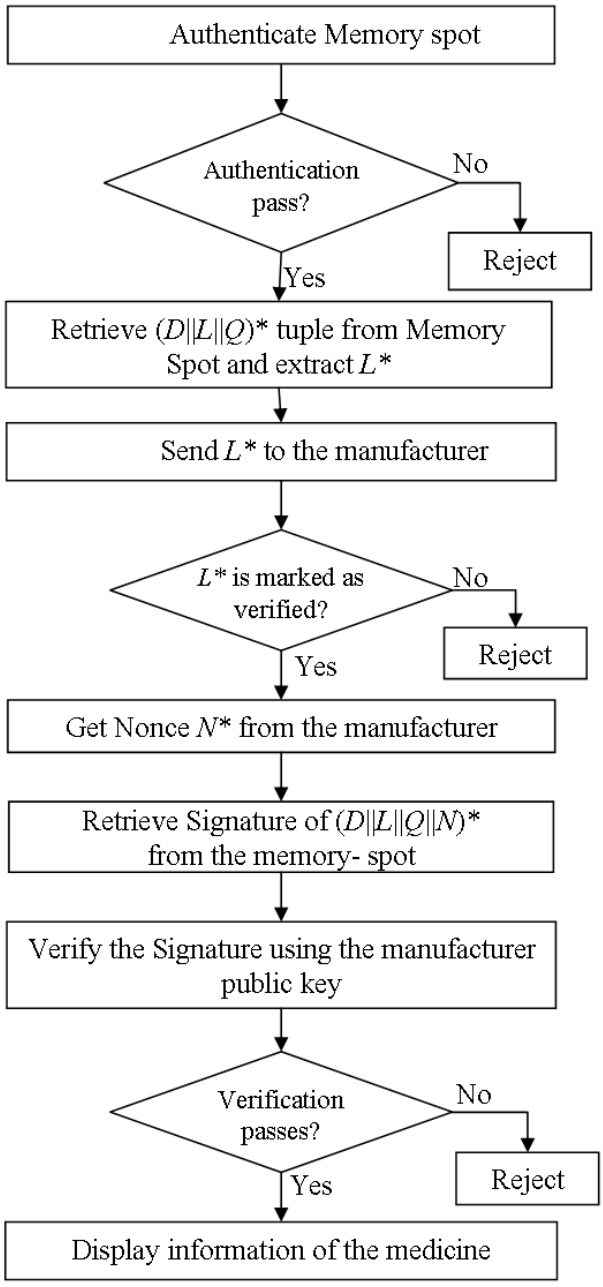

Fig. 5. End-users verification procedure

other relevant information. A failure in any one of these checks alerts the verifier that the product could be counterfeit.

3.5 Remarks

On some occasions the nonce N may not be received due to an accidental network failure or other less innocent reasons. Then, ideally the flag should not be set before there is confirmation that the returned nonce was successfully received by the querying party.

To address the issue, the login L can be into two parts, $L = L_1, L_2$. In the authentication process, the user sends L_1 only, the manufacturer returns $N' = L_2 \oplus N$, the user then computes $N = N' \oplus L_2$, and sends N back to the manufacturer. When the manufacturer sees the value N, he can be sure that the right N value has been received.

The proposed package authentication scheme allows the authenticated information to be verified only once. This seems a disadvantage, but we would like to argue that this feature is a design feature and it is suitable for pharmaceutical packages, e.g. medicines, which will be sold to and used by the end-user only once in the life time of the product. The authentication verification process can only be run when the end-user is able to access the memory spot tag which implies that the package of the product has already been broken.

4 Security Threats and Analysis

In this section, we will describe in detail existing security threats and show that the proposed solution is resistant to:

- data tampering on a memory spot tag
- memory spot tag cloning
- online attacks
- memory spot tag reuse
- impersonation attacks
- stolen memory spots attack

4.1 Data Tampering on a Memory Spot Tag

Memory spot technology provides a combinational defense on hardware and software levels. After leaving the manufacturer the memory spot tag is a read only memory with circuitry permanently disabled to prevent further writing or data alterations. On a software level, a digital signature with the manufacturer's private key is generated and stored on the memory spot. If the hardware protection proves inadequate and the data is altered, the signature will fail the verification process. As long as the private key of the manufacturer remains a secret a new signature for the amended data cannot be generated by the attacker. The end-user verifies this signature using the manufacturer's public key that he receives by a separate trusted channel, for example from the local government, FDA, National Health Service office or directly from the manufacturer.

4.2 Cloning Memory Spot Tag Attacks

This means creating a new memory spot with the same unique ID number as the original one and then copying all the data stored on the authentic memory spot onto the new one. It is a very expensive attack that can only be realized by highly organized criminals with specialist equipment, as the unique ID is provided by hardware with correspondent circuitry permanently disabled after the data has been written (read only memory), However, only one memory spot tag can be verified for a given login number through the online database, thus the real gain by counterfeiters is limited to one substituted unit per one real. The original real drugs in these circumstances have to be completely distributed through the black market without any possible verification with the manufacturer.

4.3 Online Attacks

As a referential RFID system (as for example described in [8] only returns a simple "Yes" or "No" it is theoretically simple to create a spoof site that returns correct-looking information. The memory spot system requires a correct nonce in response to a login in order to close the loop on the authentication process, which is much more difficult to create. As logins L and nonces N are sparsely distributed large random integer numbers that are hard to guess, a complete database needs to be built and populated with genuine, stolen logins and nonces; anything else will cause the signature verification to fail.

Real logins can be retrieved by scanning the drugs while in the distribution chain or by direct attack on the manufacturer database. The first scenario is hard to accomplish as memory spot has an extremely short access range and it is very easy to shield a tag from any malicious access, unless the tamper evident packaging is broken. Alternatively, the memory spot tag can be surrounded by heat sensitive ink that changes color when the tag is read (the reading process causes the tag to get warm). The second scenario is an issue of IT security and not within the scope of this paper.

4.4 Memory Spot Reuse Threat

The packaging should be made from tamper evident materials that cannot be repaired once they are broken without leaving visible marks of repair. So, we will concentrate on reuse of memory spot tags under the assumption that are already taken from their original packaging. This attack can be launched while drugs are still in a distribution chain or after a drug was used and its packaging was carelessly disposed of and subsequently maliciously collected. There are two means in our solution that prevent this attack or at least make it not-cost effective. Every unit is issued a unique login L that cannot be guessed and can be verified only once. The fact that the product is being sold and verified means that the flag in the database entry is turned on and even the whole record may be taken off line, thus rendering the read only memory spot useless. As there is no way to check the authenticity of the product without informing the

manufacturer, there is a good incentive for a customer to do so. The second measure is to make the packaging from unique signature materials, for example glass beads, using non-clonable secure seals and adding this unique signature of material to message M whose authenticity is verified by the digital signature [14]. Thus, moving the memory spot into counterfeit packaging will demand an alteration of the data inside message M, which was discussed above in "Data tampering on a memory spot tag".

4.5 Impersonation Attacks

While the design of memory spot prevents contents from one memory spot from being copied to another memory spot (cloning attack), it is still conceivable that another device could be manufactured to impersonate the memory spot.

It is technically feasible to manufacture another ASIC to clone the unique ID and the contents stored within the ROM area of a genuine memory spot, and also to physically look similar to a genuine memory spot, but such endeavor is unlikely. This is because the manufacture of an ASIC requires a substantial amount of financial investment, furthermore, the ASIC technology required to manufacture something similar to memory spot can only be provided by a few foundries in the world. This is an effective deterrent because perpetrators can easily be traced.

The defense against this threat is provided by the on-board challenge response authenticator. Secret keys can be stored in certain locations that are only accessible by the processor. The construction of memory spots does not allow these secret keys to be read by any external process once they are written. The memory spot on-board authenticator will produce a digest based on the augmentation of the challenge string issued by the reader and the said secret keys. It is appreciated that no other information besides the digest is transmitted outside memory spot; hence, no secret is ever revealed. As only the issuer knows the secret, it is virtually impossible for a third party to impersonate a memory spot device. In the case of our pharmaceutical application, the memory spot attached to each unit can be programmed with a secret (perhaps, a unique, non-derivable random number for each lot). Another set of memory spots, so called "control spots", are also programmed with the same secret. The "control spots" will then be issued to various pharmacies via a different channel (e.g. by post). A pharmacy wishing to validate the authenticity of a medicine will load the appropriate "control spot" into the reader and instruct the reader to validate the memory spot attached to the drug packaging. If the digest, reported by the "control spot", matches that reported by the memory spot attached to the drug packaging, then both spots must only have originated from the same source. Since the control spots can be trusted, the memory spot attached to the drug packaging can also be trusted.

4.6 Stolen Memory Spots

Memory spot tags can be manufactured in just a few foundries in the world and ideally they should not leave the foundry without a unique ID programmed into them. However, under some scenarios it may be that the foundry ships blank memory spot tags and it is always a possibility that there could be theft from a foundry, taking tags from the production line before their IDs are programmed. Using these blank spots any valid memory spot can be nearly completely cloned: unique ID plus contents of the memory (except the contents of the restricted access memory which is not set anyway). The only way to prevent false acceptance of the fake drugs in this case is to use unique signature materials (non-clonable) for packaging as described in [14]. The non-repeatable packaging ID forms an integral part of the data signed by the pharmaceutical company private keys. False positive identification (false acceptance) should be minimized and ideally eliminated due to the fact that patients may be put at risk of serious adverse health consequences.

If the memory spot tags are stolen after the unique ID has been programmed, this does not present a threat to the proposed solution as explained in "Cloning memory spot tag attacks". In fact, the technology is expected to be deployed by a variety of different applications and memory spots containing only a unique ID are expected to be publicly available. Stealing them therefore presents no additional threat.

5 Comparison with the Existing Solutions

"FDA's Report acknowledged the importance of using one or more authentication technologies for drug products, in particular those most likely to be counterfeited"[1]. Authentication technologies for anti-counterfeiting include measures such as color shifting inks (for example, Microtaggant® Security Ink from Microtrace [15]), holograms, fingerprints, or chemical markers embedded in a drug or its label. Generally usability studies show that users cannot accurately remember what the security features are, even for continually used things like money (like for example in [16]). Having trusted local storage of the descriptions of all the features is therefore extremely useful. In this way memory spot technology can be used to enhance existing solutions, but it also provides an authentication solution in its own right.

Referential solutions (like RFID or Call-In-Numeric-Token [8]) might benefit the manufacturer, but not so much the end-user who is left to trust a "Yes" or "No" derived in a remote location and delivered over a non-secure channel. In contrast, memory spot technology brings the authentication directly to the end-user at the point of sale, which dramatically improves security and renders IP spoofing and other attacks ineffective. Referential solutions require a verifier to retrieve a generic image of a product over the Internet, which sometimes may not be possible or practical, while memory spot's large data capacity enables all the unique features of the product to be stored locally. Our solution builds consumer trust and in the long term this will also benefit the manufacturer.

Smartcards (like Philips Mifare) have the required memory capacity, but they are physically too big to be fitted into a blister pack for example, and also they are more expensive. For some applications physical size may not be an issue.

As mentioned before, the most successful anti-counterfeiting solution in the research community is using RFID to build the supply chain security system [6]. This solution requires the involvement of many entities in the supply chain, such as multiple wholesalers. In some applications, such as pharmaceutical, building such a visible and secure chain is not easy and could be quite costly and difficult. We do not claim that our solution can cover all the security features and usability of the RFID secure supply chain. But we believe that our solution could be an alternative and supplement of the RFID secure supply chain in the pharmaceutical applications.

6 Conclusions and Future Works

Memory spot has a wide variety of market applications, ranging from vertical to consumer oriented segments. An evaluation kit has been developed and is available for demonstrations and field trials. The full solution that we have described is well suited for high value items; a subset of the features can be used to provide a more basic level of security. For example, to combat warranty fraud an on-line database with nonce and login is not required. Estimates of the component cost of the silicon for the reader are that it should be within the same region as a Bluetooth radio. However as the reader/writer shares a significant proportion of the subsystems of a WLAN chip, this could lead to substantial cost savings and an easier path to deployment in a cell-phone platform.

References

1. US, Food and Drug Administration (FDA): Combating Counterfeit Drugs, A Report of the Food and Drug Administration, February 18, 2004.
2. US, Food and Drug Administration (FDA): Combating Counterfeit Drugs: A Report of the Food and Drug Administration, Annual Update, May 18, 2005.
3. Tuyls, P., Batina, L.: RFID-tags for anti-counterfeiting. In The Cryptographers' Track at the RSA Conference 2006, San Jose, CA, USA, February 13-17, 2005, Proceedings, volume 3860 of Lecture Notes on Computer Science (LNCS), pages 115-131. Springer Verlag, 2006.
4. Staake, T., Thiesse, F., Fleisch, E.: The Potential of RFID in Anti-Counterfeiting. The 20th Annual ACM Symposium on Applied Computing Santa Fe, New Mexico, March 13 -17, 2005.
5. Lehtonen, M., Staake, T., Michahelles, F., Fleisch, E.: From Identification to Authentication - A Review of RFID Product Authentication Techniques. Workshop on RFID Security – RFIDSec 06, July 2006.
6. Staake, T., Michahelles, F., Fleisch, E., Williams, J.R., Min, H., Cole, P.H., Lee, S.G., McFarlane, D., Murai, J.: Anti-Counterfeiting and Supply Chain Security. Book chapter in Networked RFID Systems and Lightweight Cryptography - Raising Barriers to Product Counterfeiting. Cole, P.H., Ranasinghe, D.C. (Hrsg.), 2007.

7. US, Food and Drug Administration (FDA): Questions and Answers about Counterfeit Drugs, June 2, 2008.
8. Johnston, R.: An Anti-Counterfeiting Strategy Using Numeric Tokens Los Alamos National Laboratory. Int. J. of Pharmaceutical Medicine 19, 163 (2005)
9. White Paper by Philips Semiconductors: Item-level visibility in the pharmaceutical supply chain: a comparison of HF and UHF RFID technologies. TAGSYS, Texas Instruments, 2004. Available at `http://www.tagsysrfid.com/knowledge-center/upload/TAGSYS-TI-Philips-White-Paper.pdf` (June 2009)
10. Pan-European Summit for Pharmaceutical Manufacturers in the Enlarged EU, Le Mridien Piccadilly, London, February 2005.
11. Ramos, L., Holmes, B., Overby, C., McAulay, S., McEnroe, W.: Authentication, Not RFID, Will Make Drugs Safer. Forrester, July 2005. Available at `http://www.forrester.com/Research/Document/Excerpt/0,7211,36832,00.html` (June 2009)
12. Hewlett-Packard News Release: HP Unveils Revolutionary Wireless Chip that Links the Digital and Physical Worlds. Palo Alto, 2006, July. Available at `http://www.hp.com/hpinfo/newsroom/press/2006/060717a.html` (June 2009)
13. Eban, K.: Dangerous Doses, How Counterfeiters Are Contaminating America's Drug Supply. Orlando, FL: Harcourt, Inc; 2005.
14. Balinsky, H., McDonnell, E.: Anti-counterfeit packaging. International patent application PCT/EP2007 /057519, July 2007.
15. Microtaggant: Paper Solutions, Microtaggant® Security Ink, Available at `http://www.microtaggant.com/anticounterfeiting-security-ink.htm` (June 2009)
16. de Heij, H. A. M.: Feedback from the public for better banknote design. De Nederlandsche Bank (Netherlands), presentation on IS&T/SPIE 18th Annual Symposium, January 2006.