



**ADVANCED COVERT AUTHENTICATION FOR MEDICINES  
AGAINST SOPHISTICATED COUNTERFEITING**

**Background**

The pharmaceutical industry is currently facing counterfeiting, tampering and diversion threats of increasing magnitudes as well as sophistication. The motivation to fraud is there. Counterfeiters are ready to invest considerable funds and efforts in this highly profitable business. It is an open secret, already, that the profit margins achievable from fake medicines are comparable with those derived from narcotics but without having to face the same penalties when caught and brought to court. ("What's in That Pill?" Business Week, June 18, 2001). This is because in most countries, the laws against trafficking fraud medicines have not been updated to match those for narcotics even though the dangers from fraud medicines are as serious. Research into the economic impact of counterfeits within the EU concluded that 5.8% of the pharmaceutical industry's revenue – worth US\$ 1.48 B at 1998 prices – is lost to fakes ("Faking It", Manufacturing Chemist, January, 2003). The reverse side of fraud medicines is their death links. Investigation found that international bulk drug brokers were falsifying records, substituting product and replacing drugs for sale to the US pharmaceutical industry. In May 1999 to January 2000 254 adverse events were reported, including 17 deaths. Although the number of deaths is still being debated, the fact that dangerous counterfeit drugs can and have entered US healthcare system is not in dispute. One FDA investigator wrote: "Counterfeit and unapproved bulk drugs can unknowingly be turned into tablets/capsules and can reach anyone, including the President" (ibid).



The rising awareness of the pharmaceutical industry and the regulators worldwide has resulted in increasing combined efforts to fight the counterfeiting threat. The need for more powerful authenticating technologies is growing at the same rate as the counterfeiting capabilities.

### **The Required Solution Criteria**

A complete solution to cope with the fraud is challenging. It should preferably consist of a "Hierarchy of Protection" approach as described by Magali Leparc in the "New manual of Anti-Counterfeiting Solutions": The technology solution must support the legal solution, the business solution, and the enforcement efforts along the supply chain. Therefore, the required authentication system should take into consideration the following:

- **Do it covert**: Counterfeiters currently are very creative in compromising the most secured systems. The remedy is in using covert technologies on top of the traditional overt holographic or other labels. The forgers will be trapped by these invisible traps, leaving traces of their activities. This will help you screen them out as well as focusing your prevention efforts. The real authentication of a product is usually done by a powerful covert system known to a few people in your system;
- **Multiple traps**: Breaches are usually hidden to amateurish eye. We therefore recommend carefully mapping the entire supply chain, and tagging every potential entry point. Few examples are the shipping documents, consolidated



shipment labels, single package, single unit box, a blister, and the tamperproof lids;

- Single covert system: Preferably use a single covert authentication system; otherwise you may trap your own people. Your chosen system should be totally customizable to all the above-mentioned packaging levels, so that your enforcement team will use a single authentication tool;
- Zero training: Training people in a multinational company is very challenging. An authentication system that needs zero or close to zero training has great value in speed of implementation, accuracy of results and expenses;
- Fast response: The on-the-spot authentication capability of a powerful covert technology has a most substantial significance on the legal aspects of enforcements efforts. Thus, a technology that requires lab tests means additional costs and removal of the suspected object from the "crime" arena this has its legal implication for any future court action;
- Minimal human judgment: Your chosen system must be full proof. Your team must be able to distinguish between fake and genuine items under all circumstances. At the same time, the chosen system must be sophisticated enough so that no forger would be able to break it in a reasonable time and budget framework;
- High detection reliability: In order to be able to take legal actions of any kind, it is crucial to choose a reliable system that provide reliable and consistent result under various and extreme environmental conditions;
- Product liability: Authentication system must provide a reliable solution for the defined lifetime of the medicine in order to address any future product liability issues;



- Compatibility: Authentication system must be compatible with both existing production method and materials and existing security features and logistic systems. The anti-counterfeiting feature will need to be integrated into the production/packaging process with the minimum of disruptions. On the other hand, the best antifraud strategy embrace a selection of different technologies so any solution should work in parallel with existing authentication features. This also protects previous investments in anti-counterfeiting done;
- Cost performance: On top of the above, the solution should meet the customer cost expectations.

### **Covert Authentication Technologies – In Brief**

Covert authentication technologies fall into several distinct categories :

- optical tagging systems based on IF, VIS and UV additives to ink and packaging materials, including metamerics tags etc.;
- optical tagging systems based on hidden texts or images implemented in specific optical elements and/or holograms;
- magnetic tagging systems based on magnetic inks (magnetic barcodes, magnetic images);
- magnetic tagging systems based on nanomagnetic pattern recognition properties (Magneprint);
- chip based RFID (Radio Frequency IDentification) solutions;



- chipless RFID (or EMID - ElectroMagnetic IDentification) solution based on small laminated tags containing magnetic elements (Flying Null's solution, various magnetic microwire solutions);
- chipless RFID solution based on quartz or metal microresonators (InKode solution);
- chipless RFID solution based on specific sub-molecular properties of artificial substances (MicroTag solution – New Entry). MicroTag Temed Ltd, (<http://www.microtag-temed.com>) teamed up with Motorola Israel to perfect a novel authentication system. The technology is based on sophisticated physical phenomena at the sub-molecular level such as Magnetic Resonance (Nuclear Magnetic Resonance - NMR, Nuclear Quadrupole Resonance - NQR, Electron Magnetic Resonance - EMR), which were not used yet in the market and are new effects on the anti-counterfeiting arena. This technology addresses precisely the above described specifics of a modern covert security for the pharmaceutical industry;
- biomolecular systems based on the use of complex biomolecules (DNA).

The correct choice of the concrete anti-counterfeiting solution is usually determined by the balance of those advantages and disadvantages which are immanent for each technological solution. In case advantages are advertised widely by suppliers, corresponding disadvantages are usually not so clear. That is why it makes sense to be focused just on typical drawbacks :

- ✓ Optical covert solutions based on various pigments, in spite of being the most prevailing in the anti-counterfeiting market, suffer mostly from the low reliability of ID signal detection. The latter is significantly dependent on environmental



conditions such as temperature and clear line-of-sight between tag and detector. Dirt, oil, reflecting packaging layer may prevent the authentication. Another obstacle could be low compatibility of some pigments with existing printing/packaging processes. Furthermore, all these solutions are known in the market for years and may be easily replicated and/or imitated;

- ✓ Hidden texts and images cannot be considered as true machine-readable technologies. It is very hard to exclude human factor from getting decision. Moreover, these days even very smart printing and holographic technologies are available even for non-advanced forgers;
- ✓ Magnetic ink based solutions suffer the same (and even more aggravated) problems, like above mentioned optically based ones;
- ✓ Solutions on the bases of nanomagnetic pattern recognition are very sensitive to the integrity of the magnetic pattern carriers. Temperature deformations, scratches etc. may cause irreversible damage to the key ID data stored on the magnetic media. Another demerit is the need to have the entire ID database (both built in reader and on line) available for making the authenticity decision;
- ✓ At once, chip based RFID, being remote detected and possessing high data storage capacity, looks like an ideal anti-counterfeiting solution. However, three huge demerits make it practically inapplicable for anti-fraud security applications: relatively high price per tag (over 10 cents per tag in very large series), weak protection against self-forgery (chips are available in open markets, ID data may be easily simulated and stored), and so-called "fear of Big Brother" – distrust of public regarding all remote surveillance technologies;
- ✓ Chipless EMID tags (like Flying Null) are much cheaper than aforementioned RFID chips. In spite of short remote detection distances (several cm), they possess enough storage capacity to keep quite long ID keys and are, in principle,



free of “fear of Big Brother”. They are, possibly, the most prospective candidates for Track and Trace applications. Nevertheless, their applicability to secure anti-counterfeiting applications are under doubt. Firstly, the tagging method are not compatible with all standard printing\packaging technologies in use. It means that such a tag may not be introduced, for instance, into regular printing ink, paper or glue. Secondly, the reader must be connected to certain ID keys database even in the cases of simple “Yes-No” authentication, otherwise the image of ID key may be easily imitated;

- ✓ Quartz or metallic microresonators (InKode) suffer from low stability during normal printing\packaging processes, that demand using special printing machines for tagging. Another significant demerit of this solution is the tag detection in microwave frequency waveband (tens of GHz), which is forbidden for public use even at very low power levels;
- ✓ Main disadvantage of MicroTag solution is relatively short detection distances. At present the standard MicroTag reader – Prothenticator - detects the tagging substance in close proximity or at distances up to 10 mm from the reader’s probe head. Codes, stored by MicroTag technology, are orientation dependent ones and may not be recognized in remote. All these features make the MicroTag solution less attractive for direct Track and Trace applications, but remain this solution the most sophisticated for anti-fraud protection;
- ✓ DNA tags allow quite high level of anti-counterfeit protection. At the same time the reliability (self-protection) of these tags is evidently overrated. There are thousands of laboratories (at large hospitals, for example) which are able to perform corresponding DNA analysis and easily fake the DNA tag. However, the main drawback of DNA tagging solution is the lack of on-line DNA readers. Indeed, in present each DNA tag is combined with some optical (UV) tag for fast



detection of tag location. Then the tag should be sent to laboratory and pass DNA analysis there. Usually, it takes more than a day and, thus, is absolutely unacceptable for in-place anti-counterfeiting inspections.

Technologies are rarely implemented for their own sake. Any decision on the proper choice of a technological solution should be made taking into account an evaluation of costs and functionality required. We believe this article will really help decision makers to walk the optimal way.

#### Contacts:

David Keini, MicroTag Temed Ltd., Rotem Industrial Park, Arava 86800 Israel.

Email: [david@microtag-temed.com](mailto:david@microtag-temed.com)